

Название и содержание курса.

“Введение в информационную безопасность компьютерных систем”

(основы информационной безопасности).

Название и содержание курса.

Наименование модуля	Лекции	Самостоятельная работа	Краткое содержание
1. Задачи и методы обеспечения информационной безопасности	8	8	Основные понятия, цели и задачи и обеспечения информационной безопасности.
2. Теоретические основы информационной безопасности операционных систем и баз данных.	12	8	Модели и методы “теории безопасных систем”
3. Информационная безопасность вычислительных сетей.	12	8	Особенности сетевой безопасности, Вида атак и методы противодействия.
4. Проблемные вопросы обеспечения информационной безопасности автоматизированных систем и вычислительных сетей	8		Новые виды угроз, угрозы требующие новых средств и методов противодействия.
5. Методическое и организационное обеспечение информационной безопасности	8		Оценка эффективности и управление безопасностью

Госпрограмма РФ « Информационное общество (2011 - 2020 годы) » *

	2008	2011	2012	2013	2014	2015	2020
Число домашних хозяйств, имеющих широкополосный доступ в сеть Интернет, в расчете на 100 домашних хозяйств	26%	45%	47%	48%	52%	55%	80%
Доля федеральных государственных услуг, которые население может получить в электронном виде	-	39%	93%	98%	100%	100%	100%
Доля электронного документооборота между органами государственной власти в общем объеме документооборота	-	10%	15%	20%	35%	70%	70%

* выдержка

Лекция 1

**Основные понятия, термины и определения,
угрозы информационной безопасности.**

Термины и определения

ФЗ — федеральный закон

ГОСТ — государственный стандарт

ТУ — технические условия

РД - Руководящий документ

АС - автоматизированная система

ТСОИ - Технические средства обработки информации

ТС - Технические средства

ИСПДн - Информационная система обработки персональных данных

Термины и определения

Информация - сведения (сообщения, данные) независимо от формы их представления (ФЗ 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»)

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. (ФЗ 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»)

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. (ФЗ 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»)

Информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники (ФЗ 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»)

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (ФЗ 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»)

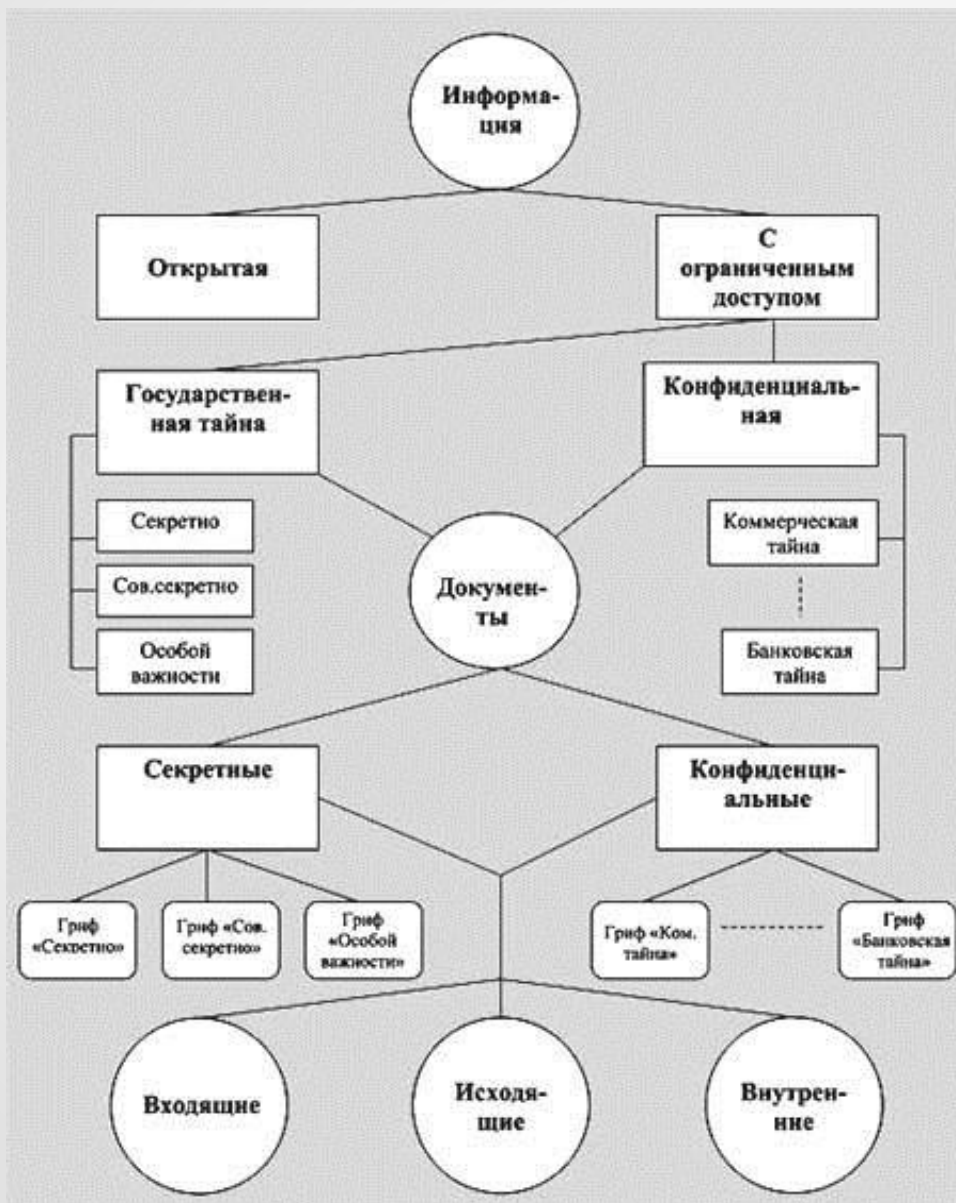
Термины и определения

Информатизация - организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов

Документированная информация (документ) - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать. (Носители информации - материальные объекты, в том числе физические поля, в которых сведения находят свое отображение в виде символов, образов, сигналов, технических решений и процессов)

Информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах, в том числе предприятий)

Термины и определения



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

Термины и определения

Безопасность - состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. (Закон РФ «О безопасности»)

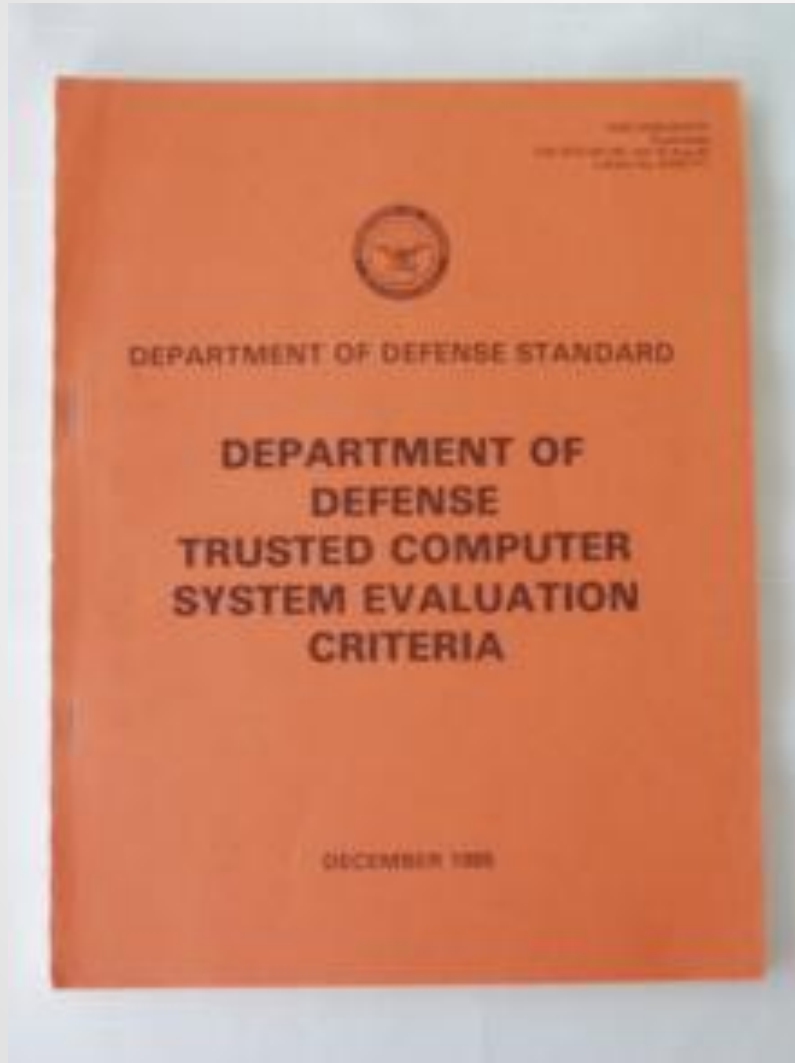
Информационная безопасность Российской Федерации - это состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства (Доктрина информационной безопасности РФ)

Безопасность информации - состояние информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается **защита информации от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации, копирования и блокирования** (Руководящий документ "Автоматизированные системы. Защита от несанкционированного доступа к информации. Термины и определения" Гостехкомиссия России 1998г.)

Термины и определения

Безопасность - состояние защищенности ?

Термины и определения



**Критерии определения
безопасности
компьютерных
систем**

***(Trusted Computer
System Evaluation
Criteria)***

Термины и определения

Информационная безопасность

Information security

Безопасность информации

Термины и определения

Информационная безопасность* — состояние (качество) **определенного** объекта (в качестве объекта может выступать информация, данные, ресурсы автоматизированной системы, автоматизированная система, информационная система предприятия, общества, государства и т. п.)

Информационная безопасность** — **защита** конфиденциальности, целостности и доступности информации.

Информационная безопасность** — деятельность, направленная на **обеспечение защищенного состояния объекта** (в этом значении чаще используется термин **«защита информации»**)

.....

*Национальный стандарт РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006).;

**Национальный стандарт РФ «Информационная технология. Практические правила управления информационной безопасностью» (ГОСТ Р ИСО/МЭК 17799—2005).;

Термины и определения

Безопасность информации (данных) — состояние защищенности информации (данных), при котором обеспечены ее (их) **конфиденциальность, доступность и целостность**.

1. Конфиденциальность: обеспечение доступа к информации только авторизованным пользователям.
2. Целостность: обеспечение достоверности и полноты информации и методов ее обработки.
3. Доступность: обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Национальный стандарт РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006).;

Термины и определения

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, **требование** не передавать такую информацию третьим лицам без согласия её обладателя»... «информация — сведения (сообщения, данные) независимо от формы их представления»

Целостность информации - **состояние защищенности** информации, характеризующееся способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения

Доступность информации - **состояние информации**, характеризующееся способностью АС обеспечивать беспрепятственный **доступ** к информации субъектов, имеющих на это полномочия

Доступ к информации (доступ) - ознакомление с информацией, её обработка, в частности копирование, модификация или уничтожение информации.

Термины и определения - уточнение

Свойства или состояние защищаемой информации или системы:

конфиденциальность информации - субъективно определяемое свойство информации, требующее введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемую способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней

целостность информации - свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию)

доступность информации - свойство системы (среды, средств и технологий ее обработки), в которой циркулирует информация, обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и требуемая готовность соответствующих подсистем к обслуживанию поступающих запросов

Термины и определения

Защита информации - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Собственником информации могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Термины и определения

Защита информации от утечки - деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.

Защита информации от разглашения - деятельность, направленная на предотвращение несанкционированного доведения защищаемой информации до потребителей, не имеющих права доступа к этой информации

Защита информации от несанкционированного доступа (НСД) - деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации

Термины и определения

Несанкционированный доступ к информации (НСД) - доступ к информации, нарушающий правила разграничения доступа **с использованием штатных средств**, предоставляемых средствами вычислительной техники или автоматизированными системами.

Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем.

В подходе Гостехкомиссии НСД является ключевым понятием и трактуется как доступ к защищаемой информации с нарушением установленных прав или правил доступа, приводящий к получению субъектом возможности ознакомления с информацией и/или воздействия на нее

Термины и определения

Троянский конь?

Вирус?

Сетевые атаки?

Это НСД?

Термины и определения

Любая **задача защиты информации** характеризуется, по крайней мере, четырьмя характеристиками, такими как **цель защиты**, **объект защиты**, **время защиты**, требуемая или максимально возможная **эффективность защиты**.

Цель защиты - это желаемый результат защиты, т.е. защиты от угроз и устранение уязвимостей.

Угроза безопасности КС - потенциально возможное действие, событие, процесс или явление, которое посредством воздействия на информацию или другие компоненты КС может прямо или косвенно привести к нанесению ущерба интересам субъектов информационных отношений.

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее.

Уязвимость информационной системы – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которые могут быть использованы для реализации угрозы безопасности информации.

Термины и определения



Термины и определения

Организация защиты информации - содержание и порядок действий, направленных на обеспечение защиты информации.

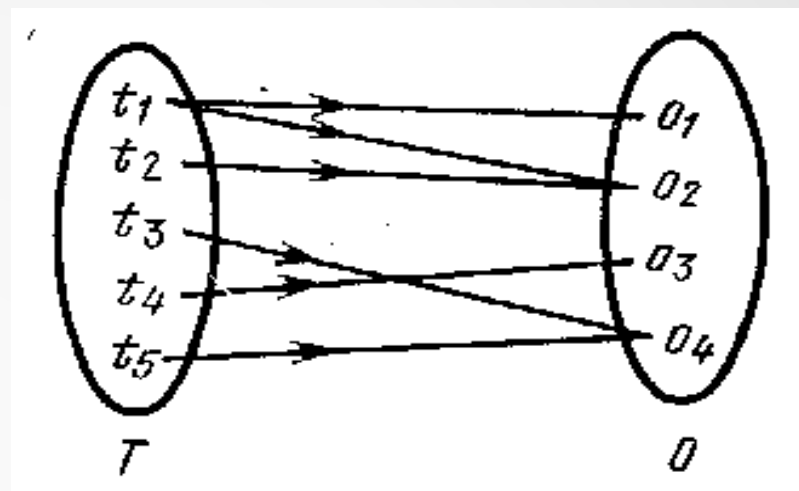
Система защиты информации - совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно - распорядительными и нормативными документами в области защиты информации

Средство защиты информации - техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации

Средство контроля эффективности защиты информации - техническое, программное средство, вещество и (или) материал, предназначенные или используемые для контроля эффективности защиты информации

Ключевые понятия

«Граф объект — угроза»



Модель с полным перекрытие Клементса

(t_i, m_j, o_k)

Ключевые понятия (IBM 1972)

- **Опознавание**
- **Управление доступом**
- **Регистрация**

Ключевые понятия (IBM 1972)

- **Контроль неизменности**
- **Изоляция**

Методы реализации

Средства защиты

- **Физические**
- **Технические**
- **Аппаратные**
- **Программные**
- **Организационные (режимные)**
- **Правовые**
- **Криптографические**

Безопасность

**Политика безопасности +
Традиционные средства защиты +
Анализ риска +
Реализация контрмер**