История и современная парадигма информационной безопасности

Вопросы

1. История развития теории и практики обеспечения информационной безопасности

2. Содержание и структура понятия информационной безопасности

3. Общая характеристика принципов, методов и механизмов обеспечения информационной безопасности

История развития теории и практики обеспечения Инф. и КБ

- Задолго до компьютерной эры. Проблемы и задачи обеспечения безопасности информации, сохранности информационных ресурсов, охраны разного рода тайн
- Военные (защита конфиденциальности)
  - Ограничение доступа
  - Разделение полномочий
- 70-е годы (появление ИС)
- Заграница
- Институт криптографии, связи и информатики (ИКСИ) Академии ФСБ России

История развития теории и практики обеспечения КБ

- ИТ - качественное изменения роли безопасности и защиты информации
  - перевод задач обеспечения безопасности информации из разряда вспомогательных, обеспечивающих, в число основных приоритетов и условий
    - возможность несанкцированного доступа
    - огромная ценность информации для корпораций
    - без значительных материальных затрат
    - Возможность мгновенного разрушения ресурсов

- 70-е годы:
  - теория безопасности компьютерной информации
    - теоретическая база,
    - программно-технические решения и
    - механизмы обеспечения безопасности при коллективной обработке общих информационных ресурсов
  - политика (методологии) и модели защиты компьютерной информации
  - модели безопасности компьютерных систем

- Начало 80-х
  - модели дискреционного (Хариссона-Руззо-Ульмана) и мандатного (Белла-ЛаПадулы) разграничения доступа
  - первые стандарты безопасности компьютерных систем. «Оранжевая книга« (1983 г.)
- 90-е годы:
  - системно-концептуальный подход к обеспечению ИБ АСОД
  - доказательный подход к проблеме гарантированности ЗИ в КС
  - теория разрушающих программных воздействий

Три взаимосвязанных, но различных направления ЗКИ

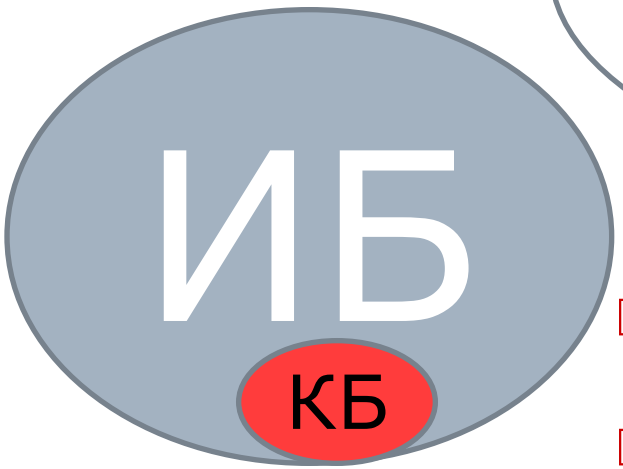
- Обеспечение
  - конфиденциальности информации,
  - целостности данных,
  - обеспечение сохранности и работоспособности данных.
- К концу 70-х годов были разработаны исходные модели безопасности КС программно-технические решения построения и функционирования защищенных компьютерных систем, в частности,
  - технологии и протоколы парольной аутентификации,
  - криптографические методы и средства защиты информации и т. д.

Триединая природа КБ

- Методы и механизмы обеспечения безопасности могут противоречивым образом влиять на различные составляющие безопасности.
- В частности методы, обеспечивающие конфиденциальность, зачастую снижают доступность информации, и наоборот.
- Внедрение защитных механизмов требует дополнительных вычислительных затрат и в большинстве случаев снижает функциональные характеристики КС.
- Системы ЗИ в КС – компромисс разработчиков между
  - обеспечением конфиденциальности, целостности данных и их доступности,
  - между защищенностью и функциональностью компьютерных систем.

Содержание и структура понятия «Информационная безопасность»

«Информационная Безопасность» - состояние защищенности информационной сферы предприятия, организации, общества, государства) от внутренних и внешних угроз



- информационная сфера (объект),
- угрозы (внутренние и внешние)
- состояние защищенности (предмет объекта)

Содержание и структура понятия «Информационная безопасность»

- «***Компьютерная система***» - *человеко-машинная система, совокупность*
  1. *Средств вычислительной техники* - электронно-программируемых технических средств обработки, хранения и представления данных,
  2. *программного обеспечения* (*ПО*), реализующего информационные технологии осуществления каких-либо функций,
  3. *Каналов связи*
  4. *информации* на различных носителях
  5. *Персонала и пользователей* системы.

Содержание и структура понятия «Компьютерная безопасность»

- «***Компьютерная безопасность» -***
  - *состояние защищенности информации (данных).*
    КС – способна противостоять внутренним и внешним угрозам
  - *безотказность (надежность) функционирования компьютерных систем*.

- Составляющими КБ выступают:
  - *безопасность информации* (данных), накапливаемых, обрабатываемых в КС, и
  - *безопасность* (безотказность, надежность) *функций КС*.

- «***Информация***» - *сведения* (*сообщения*, *данные*) *независимо от формы их представления* (ФЗ "Об информации, информационных технологиях и о защите информации")
- «***Безопасность информации***" включает три составляющих:
  - обеспечение конфиденциальности;
  - обеспечение целостности;
  - обеспечение доступности.

Конфиденциальность информации

- *Специфическое свойство отдельных категорий (видов) информации.*
- *Субъективно устанавливается ее обладателем, когда*
  - *ему может быть причинен ущерб от ознакомления с информацией неуполномоченных на то лиц,*
  - *при условии того, что обладатель принимает меры по организации доступа к информации только уполномоченных лиц*
- Обеспечение конфиденциальности –
  - обеспечение такого порядка работы с информацией, когда она известна только определенному установленному кругу лиц

Целостность информации

- *Целостность, неискаженность, достоверность, полнота, адекватность и т.д. информации -*
  - *такое ее свойство, при котором содержание и структура данных определены и изменяются только уполномоченными лицами и процессами*.

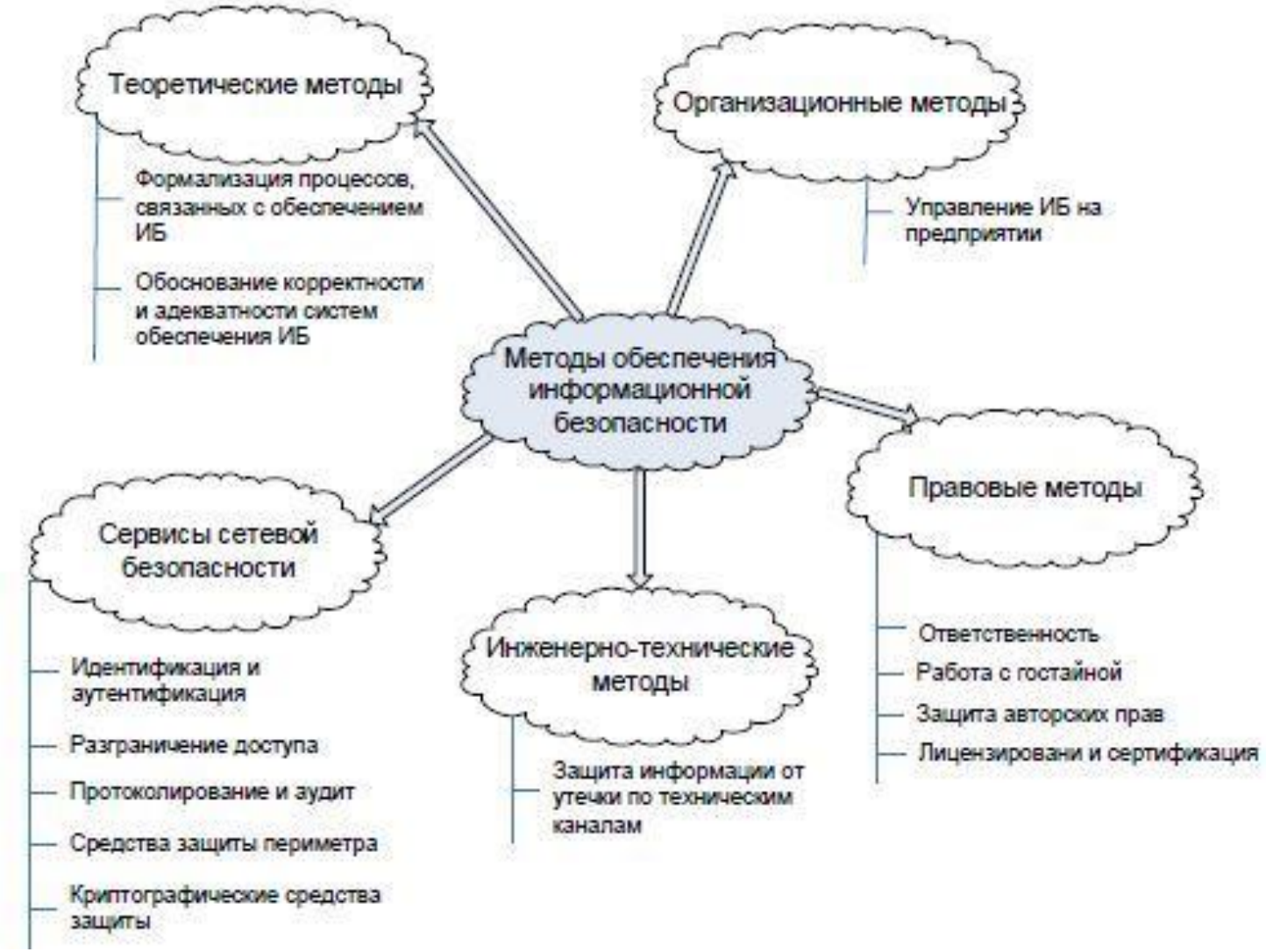
- Обеспечение безопасности информации в КС означает в т.ч. такой порядок и технологию работы с ней, когда
  - информация изменяется, модифицируется только уполномоченными лицами и
  - в процессах ее передачи, хранения не возникают (устраняются) искажения, ошибки.

Доступность информации

- Такое *свойство информации, при котором*
  - *Отсутствуют препятствия доступа к информации и закономерному ее использованию обладателем или уполномоченными лицами*.

- Обеспечивается
  - сохранностью,
  - способностью к восстановлению при сбоях и разрушениях,
  - а также в отсутствии препятствий работы с ней уполномоченных лиц.

Основные методы обеспечения ИБ



Две стороны КБ (1 => 2)

1. Безопасность (защищенность) информации
2. Безопасность (безотказность, надежность) функций компьютерных систем
   - обеспечение безотказности реализации функций
     - определяется *безотказностью оборудования* (технических средств обработки, хранения, передачи и представления информации) и
     - *безотказностью программного обеспечения* (отсутствие сбоев в работе программного обеспечения).
   1. обеспечение аутентичности реализации функций
      1. определяется *целостностью ПО* и *целостностью программно-аппаратной конфигурации* КС (параметров, настройки, состава ПО и оборудования).

Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности

Общие принципы создания и эксплуатации защищенных КС

1. Разумной достаточности
2. Целенаправленности
3. Системности
4. Комплексности
5. Непрерывности
6. Управляемости
7. Сочетания унификации и оригинальности

Принцип ***разумной достаточности***

- Внедрение в архитектуру, в алгоритмы и технологии функционирования КС защитных механизмов, функций и процедур объективно
  - вызывает дополнительные затраты,
  - издержки при создании и эксплуатации,
  - ограничивает, снижает функциональные возможности КС и параметры ее эффективности (быстродействие, задействуемые ресурсы),
  - вызывает неудобства в работе пользователям КС,
  - налагает на них дополнительные нагрузки и требования

- Поэтому защита должна быть **разумно достаточной** (на минимально необходимом уровне).

Принцип ***целенаправленности***

- Применяемые меры по
  - устранению,
  - нейтрализации (либо обеспечению снижения потенциального ущерба)
- должны быть направлены против перечня угроз (опасностей), характерных для
  - конкретной КС в
  - конкретных условиях ее создания и эксплуатации.

Принцип ***системности***

- Выбор и реализация защитных механизмов должны производиться
  - с учетом системной сути КС,
  - как организационно-технологической человеко-машинной системы, состоящей из взаимосвязанных, составляющих единое целое
    - функциональных,
    - программных,
    - технических,
    - организационно-технологических подсистем.

Принцип ***комплексности***

- При разработке системы безопасности КС необходимо использовать
  - защитные механизмы различной и наиболее целесообразной в конкретных условиях природы –
    - программно-алгоритмических,
    - процедурно-технологических,
    - нормативно-организационных,
  - и на всех стадиях жизненного цикла –
    - на этапах создания,
    - эксплуатации и
    - вывода из строя.

Принцип ***непрерывности***

- Защитные механизмы КС должны
  - функционировать в любых ситуациях в т.ч. и внештатных,
  - обеспечивая как
    - конфиденциальность,
    - целостность,
    - так и сохранность (правомерную доступность).

Принцип ***управляемости***

- Подсистема безопасности КС должна строиться как система управления –
  - объект управления (угрозы безопасности и процедуры функционирования КС),
  - субъект управления (средства и механизмы защиты),
  - среда функционирования,
  - обратная связь в цикле управления,
  - целевая функция управления (снижение риска от угроз безопасности до требуемого (приемлемого) уровня),
  - контроль эффективности (результативности) функционирования.

Принцип ***сочетания унификации и оригинальности***

1. С учетом опыта создания и применения АИС, опыта обеспечения безопасности КС
   - должны применяться максимально проверенные, стандартизированные и унифицированные архитектурные, программно-алгоритмические, организационно-технологические решения.
2. С учетом динамики развития ИТ, диалектики средств нападения и развития
   - должны разрабатываться и внедряться новые оригинальные архитектурные, программно-алгоритмические, организационно-технологические решения, обеспечивающие безопасность КС в новых условиях угроз, с минимизацией затрат и издержек, повышением эффективности и параметров функционирования КС, снижением требований к пользователям.

Систематика методов и механизмов обеспечения КБ

- Продолжение следует …

Угрозы безопасности компьютерных систем и информационно-коммуникационных технологий