Литература по курсу

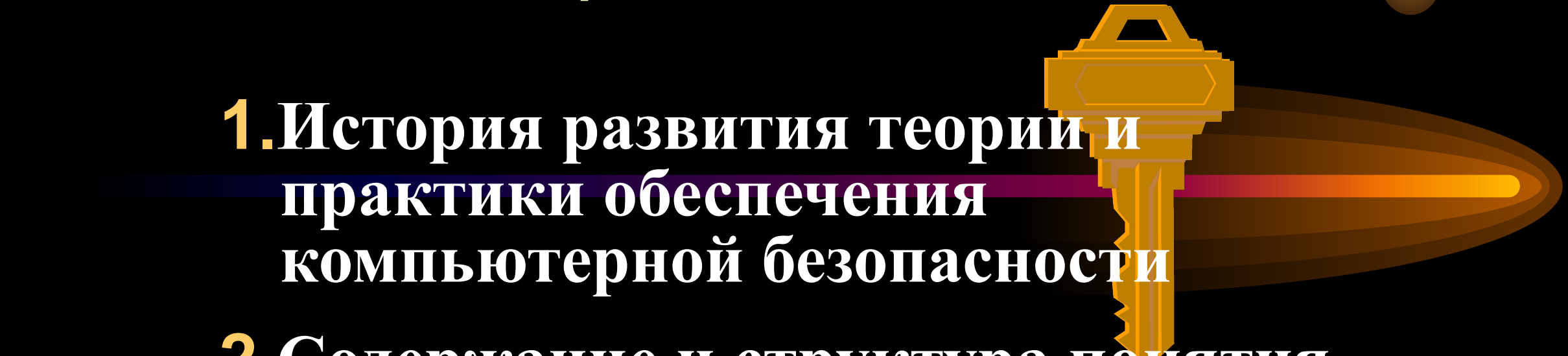
1. **Хоффман Л.** Современные методы защиты информации. М.:Сов. радио, 1980. – 264с.
2. **Грушо А.А.,Тимонина Е.Е.** Теоретические основы защиты информации. М.:Яхтсмен, 1996. - 192с.
3. **Теория и практика обеспечения информационной безопасности** / Под ред. П.Д. **Зегжды**. М.:Яхтсмен, 1996. - 302с
4. **Прокопьев И.В., Шрамков И.Г., Щербаков А.Ю.** Введение в теоретические основы компьютерной безопасности : Уч. пособие. М., 1998.- 184с.
5. **Зегжда Д.П.,Ивашко А.М.** Основы безопасности информационных систем. - М.:Горячая линия - Телеком, 2000. - 452с.
6. Теоретические основы компьютерной безопасности: Учеб. пособие для вузов / **П.Н. Девянин, О.О.Михальский, Д.И.Правиков** и др.- М.: Радио и Связь, 2000. - 192с.
8. **Щербаков А.Ю.** Введение в теорию и практику компьютерной безопасности. М.: издатель Молгачев С.В.- 2001- 352 с.
9. **Гайдамакин Н.А.** Разграничение доступа к информации в компьютерных системах. - Екатеринбург: изд-во Урал. Ун-та, 2003. – 328 с.
10. **Корт С.С.** Теоретические основы защиты информации: Учебное пособие. – М.: Гелиос АРВ, 2004. – 240 с.
11. **Девянин П.Н.** Модели безопасности компьютерных систем: Учеб. пособие. – М.: Изд.центр «Академия», 2005. – 144 с.

Тема 1. Основы теории компьютерной безопасности

Лекция 1.1.

Содержание и основные понятия компьютерной безопасности

Учебные вопросы:



1. История развития теории и практики обеспечения компьютерной безопасности
2. Содержание и структура понятия компьютерной безопасности
3. Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности

1. История развития теории и практики обеспечения компьютерной безопасности

Защита информации – проблема с древнейших времен

Специфика компьютерной формы информации:

- возможность получения доступа к большим объемам информации в локальном физическом сосредоточении
- возможность быстрого или мгновенного копирование огромн объемов информации и, как правило, без следов
- возможность быстрого или мгновенного разрушения или искажения огромных объемов информации

провоцирует на посягательство

в результате – КС и ИБ – неотделимые понятия

Защита (обеспечение) безопасности информации – не просто вспомогательная, но одна из главных (основных) функций КС при их создании

Основные этапы развития теории и практики КБ:

Этап	Год	Основные факторы	Содержание
Начальный	60-е - 70-е г.г.	•Появление ЭВМ 3-го поколения •Начало примен-я ЭВМ для инф. обеспеч-я крупн. предпр-й и орг-й	•Начало теоретич. иссл. проблем защиты КИ (АДЕПТ-50, 1967г.) •Исследование и первые реализации технолог. аспектов защиты инф-и (парольные системы аутентификации) •"Открытие" криптографии во внегосударственной сфере (однако 1-е работы К.Шеннона в 1949г.)
2-й этап	70-е - нач. 80-х г.г.	•Широкое внедр. ЭВМ в инф.обесп. не только крупн., но средн. предпр. •Персонализация СВТ •Внедр. ПЭВМ в офисн., фин/хоз/ экон. деят-ть •Появл. на базе ПЭВМ систем лок. инф. коммун.	•Интенсивные теоретич. исследования по формальным моделям безопасности: -Хоффман(1970-1974 г.г.) -Хартсон (1975г.) -Харрисон, Рузо, Ульман (1975г.) -Белл, ЛаПадула (1975г.-1976г.) •Опубл-е в США стандарта DES (1977г.) •Интенс-е теор. иссл-я в сфере нессиметр. криптографии: -У.Диффи, М.Хеллман (1976г.) -стандарт RSA - Р.Райвест, А.Шамир А.Адлеман (1978г.) •"Оранжевая книга" (1983г.) •MMS-модель (1984г.) •ГОСТ 28147-89

Основные этапы развития теории и практики КБ:

Эт ап	Год ы	Основные факторы	Содержание
3-й этап	ко-нец 80-х - 90-е г.г.	•Полная компьюте-ризация всех сфер деятельности •Повсеместн. исп. ПК, в т.ч. и как ср. инф. коммун. •Возникн. и стрем. разв. глоб. инф.-компь. инфраструктуры (сети Интернет) •Возникновения и развитие "Инфор-мационного" зако-нодательства	•Дальн. разв. формальных моделей и техноло-гий защиты информации •Переход на "защищенность" при разработке коммерческих КС: -ОС -СУБД •Появление спец. проблемы КБ – **компьютер-ных вирусов** (термин ввел Ф.Коэн, 1984) •Развитие национальных и международных стандартов защищенности КС •Широкое внедрение криптографических средств защиты информации: -для хранения и передачи КИ -в архитектуру КС -в процедуры аутентификации (появл. криптограф. протоколов) •Теорет. иссл. и реализация практ. систем обеспечения целостности КИ (появления стандартов и систем ЭЦП) •Появление "компьютерной" преступности

Основные этапы развития теории и практики КБ:

Отечественная школа КБ

В.А.Герасименко - *1991г.*, модель системно-концептуального подхода к безопасности

Грушо А.А., Тимонина Е.Е. – *1996г.,* гарантированность защищенности АС как математическое доказательство гарантированного выполнения априорно заданной политики без-ти

Расторгуев С.П., ***начало 90-х г.г. -*** теория разрушающих программных воздействий, ***середина 90-х г.г. -*** теория информационного противоборства

Щербаков А.Ю. – ***90-е г.г.,*** субъектно-объектная модель изолированной программной среды

СПб школа **Зегжды П.Д.** – ***середина 90-х г.г.,*** таксонометрия изъянов безопасности КС

Школа **ИКСИ** (**Б.А.Погорелов, А.П.Коваленко**) – ***конец 90-х г.г.,*** государственные образовательные стандарты подготов-ки специалистов в сфере компьютерной безопасности

2. Содержание и структура понятия компьютерной безопасности

Иерархия понятий:

Безопасность

Информационная *Безопасность*

Компьютерная *Безопасность*

Безопасность компьютерной информации

Методологическая база - понятие ***безопасности***
(з-н "О безопасности", 1993г.)

- состояние ***защищенности*** жизненно важных интересов личности, общества и государства от внутренних и внешних ***угроз***

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

Компьютерная безопасность – состояние защищенности (безопасность) информации в компьютерных системах и безотказность (надежность) функционирования компьютерных систем

2. Содержание и структура понятия компьютерной безопасности

Компьютерная безопасность

Безопасность информации в КС

- Обеспечение конфиденциальности информации
- Обеспечение целостности информации
- Обеспечение доступности информации

- такое свойство информации, при котором отсутствуют препятствия доступа к информации и закономерному ее использованию собственником или уполномоченными лицами процессами

принимает меры по организации доступа к информации только уполномоченных лиц

Безотказность (надежность) функционирования КС

- Обеспечение аутентичности реализации функций
- Обеспечение безотказности реализации функций

- Обеспечение целостности параметров ПО
- Обеспечение целостности ПО
- Обеспечение безотказности ПО
- Обеспечение безотказности оборудования

2. Содержание и структура понятия компьютерной безопасности

Безопасность информации

- состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации от утечки, хищения, утраты, несанкционированного уничтожения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п.

3. Общая характеристика принципов, методов и механизмов

Общие принципы обеспечения компьютерной безопасности

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 КС, 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)

Целенаправленности

-устранение, нейтрализация (либо обеспечение снижения потенциального ущерба) конкретного перечня угроз (опасностей), характерных для конкретной КС в конкретных условиях ее создания и эксплуатации

Системности

-выбор защитных механизмов с учетом системной сути КС, как организационно-технологической человеко-машинной системы, состоящей из взаимосвязанных, составляющих единое целое функциональных, программных, технических, организационно-технологических подсистем

Комплексности

-выбор защитных механизмов 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

3. Общая характеристика принципов, методов и механизмов

Общие принципы обеспечения компьютерной безопасности

Непрерывности

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

Управляемость

-система защиты КС строится 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

Сочетания унификации и оригинальности

-с одной стороны с учетом опыта создания и применения КС, опыта обеспечения безопасности КС должны применяться максимально проверенные, стандартизированные и унифицированные архитектурные, программно-алгоритмические, организационно-технологические решения,

-с другой стороны, с учетом динамики развития ИТ, диалектики средств нападения и защиты 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

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

Систематика методов и механизмов обеспечения КБ

Основного характера (прямого действия)

Общесистемного характера

Инфраструктурного характера

- Управление (контроль) конфигурацией
- Управление сеансами
- Управление удаленным доступом с раб. станций
- Управление сетевым соединениями

Общеархитектурного характера

- Идентификация аутентификация пользователей, устройств, данных
- Управление памятью, потоками, изоляция процессов
- Управление транзакциями

- Управление инфраструктурой сертификатов криптоключей

Непосредственного действия

- Разграничение доступа к данным
- Контроль, управление информационной структурой данных
- Контроль ограничений целостности данных
- Шифрование данных
- ЭЦП данных
- Защита/удаление остаточной информации на носителях данных и в освобождаемых областях оперативной памяти

конфиденциальность

целостность

доступность

Обеспечивающего (профилактирующего) характера

- Протоколирование, аудит событий
- Резервирование данных, журнализация процессов изменения данных
- Профилактика носителей данных
- Учет/контроль носителей данных
- Нормативно-организационная регламентация использования КС
- Обучение. нормативно-административное побуждение и принуждение пользователей по вопросам ИБ

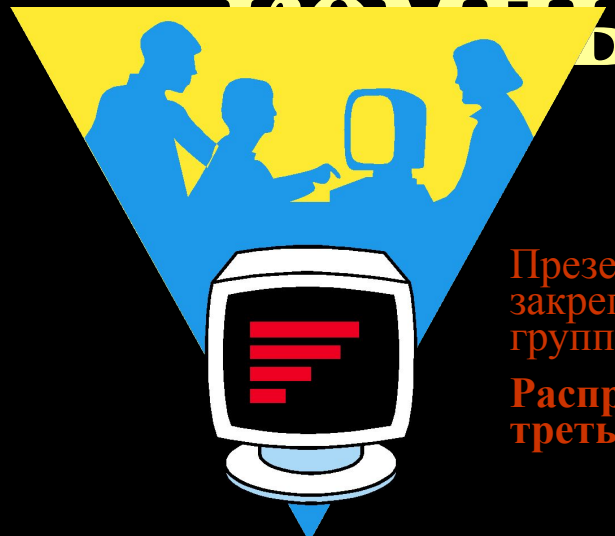
ГОС 075200 «Компьютерная безопасность»

ОПД.Ф.10 «Теоретические основы компьютерной безопасности»

Тема 1. Исходные положения теории компьютерной безопасности

Лекция 1.2.

Угрозы безопасности в компьютерных системах



Презентация предназначена для отработки и закрепления лекционного материала студентами группы КБ МатМех УрГУ.