

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Институт физики



УТВЕРЖДАЮ

Проректор
по образовательной деятельности КФУ
Проф. Минзарипов Р.Г.

"__" _____ 20__ г.

Программа дисциплины

Теоретические основы компьютерной безопасности Б3.В.4

Направление подготовки: 090900.62 - Информационная безопасность

Профиль подготовки: Информационная безопасность автоматизированных систем

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Автор(ы):

Насыров И.А.

Рецензент(ы):

Гумеров Р.И.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Овчинников М. Н.

Протокол заседания кафедры No ____ от "____" _____ 201__ г

Учебно-методическая комиссия Института физики:

Протокол заседания УМК No ____ от "____" _____ 201__ г

Регистрационный No

Казань
2015

Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре основной образовательной программы
3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля
4. Структура и содержание дисциплины/ модуля
5. Образовательные технологии, включая интерактивные формы обучения
6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов
7. Литература
8. Интернет-ресурсы
9. Материально-техническое обеспечение дисциплины/модуля согласно утвержденному учебному плану

Программу дисциплины разработал(а)(и) доцент, к.н. (доцент) Насыров И.А. Кафедра радиоэлектроники Отделение радиофизики и информационных систем , Igor.Nasyrov@kpfu.ru

1. Цели освоения дисциплины

Дисциплина "Теоретические основы компьютерной безопасности" имеет целью обучить студентов принципам и методам защиты информации, комплексного проектирования, построения, обслуживания и анализа защищенных автоматизированных систем (АС), а также содействовать фундаментализации образования, формированию научного мировоззрения и развитию системного мышления. Задачи дисциплины - дать основы:

- устройства и принципов функционирования защищенных АС,
- методологии проектирования и построения защищенных АС,
- критериев и методов оценки защищенности АС,
- средств и методов несанкционированного доступа (НСД) к информации АС.

2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " БЗ.В.4 Профессиональный" основной образовательной программы 090900.62 Информационная безопасность и относится к вариативной части. Осваивается на 3 курсе, 5 семестр.

Знания и практические навыки, полученные из курса "Теоретические основы компьютерной безопасности", используются обучаемыми при изучении естественнонаучных дисциплин, при разработке курсовых и дипломных работ.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-1 (общекультурные компетенции)	способностью осознавать необходимость соблюдения Конституции Российской Федерации, прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма
ОК-2 (общекультурные компетенции)	способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм
ОК-5 (общекультурные компетенции)	способностью к кооперации с коллегами, работе в коллективе
ОК-6 (общекультурные компетенции)	способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность
ОК-7 (общекультурные компетенции)	способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства
ПК-3 (профессиональные компетенции)	способностью использовать нормативные правовые документы в своей профессиональной деятельности

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-4 (профессиональные компетенции)	способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности
ПК-8 (профессиональные компетенции)	способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия

В результате освоения дисциплины студент:

1. должен знать:

- методологические и технологические основы комплексного обеспечения безопасности АС,
- угрозы и методы нарушения безопасности АС,
- формальные модели, лежащие в основе систем защиты АС,
- стандарты по оценке защищенности АС и их теоретические основы,
- методы и средства реализации защищенных АС,
- методы и средства верификации и анализа надежности защищенных АС;

2. должен уметь:

- проводить анализ АС с точки зрения обеспечения компьютерной безопасности,
- разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и их теоретические основы,
- применять стандарты по оценке защищенности АС при анализе и проектировании систем защиты информации в АС,
- реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищенности АС;

3. должен владеть:

навыками:

- работы с АС распределенных вычислений и обработки информации;
- работы с документацией АС,
- использования критериев оценки защищенности АС,
- построения формальных моделей систем защиты информации АС.

4. должен демонстрировать способность и готовность:

- проводить анализ АС с точки зрения обеспечения компьютерной безопасности,
- разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и их теоретические основы,
- применять стандарты по оценке защищенности АС при анализе и проектировании систем защиты информации в АС,
- реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищенности АС;

иметь навыки:

- работы с АС распределенных вычислений и обработки информации;
- работы с документацией АС,
- использования критериев оценки защищенности АС,
- построения формальных моделей систем защиты информации АС.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 4 зачетных(ые) единиц(ы) 144 часа(ов).

Форма промежуточного контроля дисциплины экзамен в 5 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Структура теории компьютерной безопасности. Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ. Ценность информации. Аддитивная модель. Порядковая шкала. Решетка ценности.	5	1	4	0	0	устный опрос
2.	Тема 2. Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы данных.	5	2	4	0	0	устный опрос

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
3.	Тема 3. Основные виды атак на АС. Классификация основных атак на АС и вредоносных программ.	5	3	4	0	0	устный опрос
4.	Тема 4. Методология построения систем защищенных АС. Построение систем защиты от угрозы нарушения конфиденциальности информации. Организационно режимные меры. Защита от НСД. Построение парольных систем. Криптографические методы защиты. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.	5	4-6	6	0	14	отчет
5.	Тема 5. Построение систем защиты от угрозы нарушения целостности информации. Организационно-технологические меры защиты. Защита целостности программно-аппаратной среды. Основные методы защиты памяти. Цифровая подпись. Защита от угрозы целостности на уровне содержания информации.	5	7-8	4	0	8	отчет

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
6.	Тема 6. Методология обследования и проектирования защиты АС. Применение иерархического метода для построения защищенной АС. Исследование корректности реализации и ме-тоды верификации АС. Теория безопасных систем (ТСВ).	5	9	4	0	0	устный опрос
7.	Тема 7. Политика безопасности. Понятие политики безопасности Политика (стратегия) безопасности. Дискреционная политика разграничения доступа. Мандатная (полномочная) политика разграничения доступа. Разработка и реализация политики безопасности.	5	10	4	0	0	устный опрос
8.	Тема 8. Модели безопасности. Описание систем защиты с помощью матрицы доступа. Модель Харрисона-Руззо-Ульмана (HRU). Разрешимость проблемы безопасности. Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant, анализ информационных каналов. Описание модели Белла-Лападулы (BL).	5	11	4	0	0	устный опрос

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
9.	Тема 9. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ. Классификация СВТ по документам Гостехкомиссии. Классификация АС по документам Гостехкомиссии, требования классов защиты.	5	12	2	0	0	контрольная точка
10.	Тема 10. Защита информации от внутренних угроз. Защищаемый периметр информации. Предотвращение утечек (Data Loss Prevention, DLP) - технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек. Решения SearchInform.	5	13-17	0	0	14	письменная работа
.	Тема . Итоговая форма контроля	5		0	0	0	экзамен
	Итого			36	0	36	

4.2 Содержание дисциплины

Тема 1. Структура теории компьютерной безопасности. Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ. Ценность информации. Аддитивная модель. Порядковая шкала. Решетка ценности.

лекционное занятие (4 часа(ов)):

Структура теории компьютерной безопасности. Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ. Ценность информации. Аддитивная модель. Порядковая шкала. Решетка ценности.

Тема 2. Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы данных.

лекционное занятие (4 часа(ов)):

Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы данных.

Тема 3. Основные виды атак на АС. Классификация основных атак на АС и вредоносных программ.

лекционное занятие (4 часа(ов)):

Основные виды атак на АС. Классификация основных атак на АС и вредоносных программ.

Тема 4. Методология построения систем защищенных АС. Построение систем защиты от угрозы нарушения конфиденциальности информации. Организационно режимные меры. Защита от НСД. Построение парольных систем. Криптографические методы защиты. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.

лекционное занятие (6 часа(ов)):

Методология построения систем защищенных АС. Построение систем защиты от угрозы нарушения конфиденциальности информации. Организационно режимные меры. Защита от НСД. Построение парольных систем. Криптографические методы защиты. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.

лабораторная работа (14 часа(ов)):

Системы с симметричными ключами. Особенности реализации.

Тема 5. Построение систем защиты от угрозы нарушения целостности информации. Организационно-технологические меры защиты. Защита целостности программно-аппаратной среды. Основные методы защиты памяти. Цифровая подпись. Защита от угрозы целостности на уровне содержания информации.

лекционное занятие (4 часа(ов)):

Построение систем защиты от угрозы нарушения целостности информации. Организационно-технологические меры защиты. Защита целостности программно-аппаратной среды. Основные методы защиты памяти. Цифровая подпись. Защита от угрозы целостности на уровне содержания информации.

лабораторная работа (8 часа(ов)):

Системы с несимметричными ключами. Особенности реализации.

Тема 6. Методология обследования и проектирования защиты АС. Применение иерархического метода для построения защищенной АС. Исследование корректности реализации и методы верификации АС. Теория безопасных систем (ТСВ).

лекционное занятие (4 часа(ов)):

Методология обследования и проектирования защиты АС. Применение иерархического метода для построения защищенной АС. Исследование корректности реализации и методы верификации АС. Теория безопасных систем (ТСВ).

Тема 7. Политика безопасности. Понятие политики безопасности Политика (стратегия) безопасности. Дискреционная политика разграничения доступа. Мандатная (полномочная) политика разграничения доступа. Разработка и реализация политики безопасности.

лекционное занятие (4 часа(ов)):

Политика безопасности. Понятие политики безопасности Политика (стратегия) безопасности. Дискреционная политика разграничения доступа. Мандатная (полномочная) политика разграничения доступа. Разработка и реализация политики безопасности.

Тема 8. Модели безопасности. Описание систем защиты с помощью матрицы доступа. Модель Харрисона-Руззо-Ульмана (HRU). Разрешимость проблемы безопасности. Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant, анализ информационных каналов. Описание модели Белла-Лападулы (BL).

лекционное занятие (4 часа(ов)):

Модели безопасности. Описание систем защиты с помощью матрицы доступа. Модель Харрисона-Руззо-Ульмана (HRU). Разрешимость проблемы безопасности. Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant, анализ информационных каналов. Описание модели Белла-Лападулы (BL).

Тема 9. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ. Классификация СВТ по документам Гостехкомиссии. Классификация АС по документам Гостехкомиссии, требования классов защиты.

лекционное занятие (2 часа(ов)):

Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ. Классификация СВТ по документам Гостехкомиссии. Классификация АС по документам Гостехкомиссии, требования классов защиты.

Тема 10. Защита информации от внутренних угроз. Защищаемый периметр информации. Предотвращение утечек (Data Loss Prevention, DLP) - технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек. Решения SearchInform.

лабораторная работа (14 часа(ов)):

Установка и первоочередная настройка программного комплекса SearchInform. Принципы использования программного комплекса SearchInform для мониторинга утечек конфиденциальной информации. Настройка программного комплекса SearchInform для контроля содержимого экранов пользователей и поиска конфиденциальной информации без проведения синтаксического анализа. Настройка программного комплекса SearchInform для поиска конфиденциальной информации на основе подобия текстовых фрагментов. Формирование регулярных выражений и настройка системы перехвата передаваемой информации.

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Структура теории компьютерной безопасности. Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ. Ценность информации. Аддитивная модель. Порядковая шкала. Решетка ценности.	5	1	подготовка к устному опросу	2	устный опрос
2.	Тема 2. Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы данных.	5	2	подготовка к устному опросу	2	устный опрос

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
3.	Тема 3. Основные виды атак на АС. Классификация основных атак на АС и вредоносных программ.	5	3	подготовка к устному опросу	2	устный опрос
5.	Тема 5. Построение систем защиты от угрозы нарушения целостности информации. Организационно-технологические меры защиты. Защита целостности программно-аппаратной среды. Основные методы защиты памяти. Цифровая подпись. Защита от угрозы целостности на уровне содержания информации.	5	7-8	подготовка к отчету	12	отчет
6.	Тема 6. Методология обследования и проектирования защиты АС. Применение иерархического метода для построения защищенной АС. Исследование корректности реализации и методы верификации АС. Теория безопасных систем (ТСВ).	5	9	подготовка к устному опросу	2	устный опрос
7.	Тема 7. Политика безопасности. Понятие политики безопасности Политика (стратегия) безопасности. Дискреционная политика разграничения доступа. Мандатная (полномочная) политика разграничения доступа. Разработка и реализация политики безопасности.	5	10	подготовка к устному опросу	2	устный опрос

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
8.	Тема 8. Модели безопасности. Описание систем защиты с помощью матрицы доступа. Модель Харрисона-Руззо-Ульмана (HRU). Разрешимость проблемы безопасности. Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant, анализ информационных каналов. Описание модели Белла-Лападулы (BL).	5	11	подготовка к устному опросу	2	устный опрос
9.	Тема 9. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ. Классификация СВТ по документам Гостехкомиссии. Классификация АС по документам Гостехкомиссии, требования классов защиты.	5	12	подготовка к контрольной точке	2	контрольная точка

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
10.	Тема 10. Защита информации от внутренних угроз. Защищаемый периметр информации. Предотвращение утечек (Data Loss Prevention, DLP) - технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек. Решения SearchInform.	5	13-17	подготовка к письменной работе	10	письменная работа
	Итого				36	

5. Образовательные технологии, включая интерактивные формы обучения

Компьютерный класс с предустановленным программным обеспечением SearchInform и Microsoft VisualStudio.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Тема 1. Структура теории компьютерной безопасности. Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ. Ценность информации. Аддитивная модель. Порядковая шкала. Решетка ценности.

устный опрос , примерные вопросы:

Структура теории компьютерной безопасности. Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ. Ценность информации. Аддитивная модель. Порядковая шкала. Решетка ценности.

Тема 2. Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы данных.

устный опрос , примерные вопросы:

Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы данных.

Тема 3. Основные виды атак на АС. Классификация основных атак на АС и вредоносных программ.

устный опрос , примерные вопросы:

Основные виды атак на АС. Классификация основных атак на АС и вредоносных программ.

Тема 4. Методология построения систем защищенных АС. Построение систем защиты от угрозы нарушения конфиденциальности информации. Организационно режимные меры. Защита от НСД. Построение парольных систем. Криптографические методы защиты. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.

Тема 5. Построение систем защиты от угрозы нарушения целостности информации. Организационно-технологические меры защиты. Защита целостности программно-аппаратной среды. Основные методы защиты памяти. Цифровая подпись. Защита от угрозы целостности на уровне содержания информации.

отчет , примерные вопросы:

Построение систем защиты от угрозы нарушения целостности информации. Организационно-технологические меры защиты. Защита целостности программно-аппаратной среды. Основные методы защиты памяти. Цифровая подпись. Защита от угрозы целостности на уровне содержания информации.

Тема 6. Методология обследования и проектирования защиты АС. Применение иерархического метода для построения защищенной АС. Исследование корректности реализации и методы верификации АС. Теория безопасных систем (ТСВ).

устный опрос , примерные вопросы:

Методология обследования и проектирования защиты АС. Применение иерархического метода для построения защищенной АС. Исследование корректности реализации и методы верификации АС. Теория безопасных систем (ТСВ).

Тема 7. Политика безопасности. Понятие политики безопасности Политика (стратегия) безопасности. Дискреционная политика разграничения доступа. Мандатная (полномочная) политика разграничения доступа. Разработка и реализация политики безопасности.

устный опрос , примерные вопросы:

Политика безопасности. Понятие политики безопасности Политика (стратегия) безопасности. Дискреционная политика разграничения доступа. Мандатная (полномочная) политика разграничения доступа. Разработка и реализация политики безопасности.

Тема 8. Модели безопасности. Описание систем защиты с помощью матрицы доступа. Модель Харрисона-Руззо-Ульмана (HRU). Разрешимость проблемы безопасности. Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant, анализ информационных каналов. Описание модели Белла-Лападулы (BL).

устный опрос , примерные вопросы:

Модели безопасности. Описание систем защиты с помощью матрицы доступа. Модель Харрисона-Руззо-Ульмана (HRU). Разрешимость проблемы безопасности. Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant, анализ информационных каналов. Описание модели Белла-Лападулы (BL).

Тема 9. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ. Классификация СВТ по документам Гостехкомиссии. Классификация АС по документам Гостехкомиссии, требования классов защиты.

контрольная точка , примерные вопросы:

Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ. Классификация СВТ по документам Гостехкомиссии. Классификация АС по документам Гостехкомиссии, требования классов защиты.

Тема 10. Защита информации от внутренних угроз. Защищаемый периметр информации. Предотвращение утечек (Data Loss Prevention, DLP) - технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек. Решения SearchInform.

письменная работа , примерные вопросы:

ащита информации от внутренних угроз. Защищаемый периметр информации.
Предотвращение утечек (Data Loss Prevention, DLP) - технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек. Решения SearchInform.

Тема . Итоговая форма контроля

Примерные вопросы к экзамену:

Примерный перечень экзаменационных вопросов

1. Основные понятия информационной безопасности.
2. Автоматизированная система обработки информации. Представление информации в АС.
3. Базовые свойства информации
4. Допуск к информации. Базовые понятия
5. Определение угрозы безопасности для АС. Противодействие угрозам безопасности
6. Классификация возможных угроз информационной безопасности АС. Важные свойства информации и систем ее обработки.
7. Уровни доступа к информации. Анализ угроз информационной безопасности.
8. Базовая эталонная модель взаимодействия открытых систем
9. Протокол. Сеть как набор протоколов
10. Стек протоколов TCP/IP. Соответствие уровней стека TCP/IP уровням модели OSI.
11. IP адресация. Классы IP сетей. Характеристики классов IP-адресов. Выделенные IP-адреса.
12. Шлюзы и мосты. Маска подсети. Подсети - первый бастион защиты.
13. Интернет протоколы: Протокол пересылки файлов FTP; Протокол Telnet; Протокол SNMP; Протокол SMTP; Сетевая файловая система NFS; Протокол передачи гипертекста (HTTP); Сервис DNS.
14. Схема инкапсуляции данных в стеке протоколов TCP/IP. ARP-таблица.
15. Проблемы безопасности IP-сетей. Угрозы безопасности IP-сетей. Анализ угроз сетевой безопасности.
16. Сетевые атаки: Подслушивание; Изменение данных; Анализ сетевого трафика; Подмена доверенного субъекта; Посредничество; Атака man-in-the-middle; Перехват сеанса; Парольные атаки; Угадывание ключа; Атаки на уровне приложений; Отказ в обслуживании (Denial of Service, DoS); Сетевая разведка; Злоупотребление доверием.
17. Угрозы и уязвимости проводных корпоративных информационных систем.
18. Угрозы и уязвимости беспроводных сетей. Точки доступа в беспроводных сетях. Вещание радиомаяка.
19. Способы обеспечения информационной безопасности. Комплексный подход. Необходимость применения стандартов
20. Криптография. Шифрование с закрытым ключом. Понятие диффузии и конфузии. Структура алгоритма симметричного шифрования. Криптоанализ. Используемые критерии при разработке алгоритмов. Сеть Фейстеля. Понятие слабого ключа.
21. Асимметричное шифрование. Основные принципы построения криптосистем с открытым ключом. Основные алгоритмы построения систем с открытым ключом.
22. Электронная цифровая подпись. Цель аутентификации электронных документов. Формат электронной цифровой подписи. Хэш-функция. Одно направленные Хэш-функции. Основы построения хэш-функций.

23. Технологии межсетевых экранов. Функции МЭ. Классификация МЭ. Фильтрация трафика. Критерии анализа информационного потока. Выполнение функций посредничества. Способы разграничения доступа к ресурсам внешней/внутренней сети. Кэширование данных. Особенности функционирования МЭ на различных уровнях модели OSI. Варианты исполнения МЭ. Схемы сетевой защиты на базе МЭ. Формирование политики межсетевого взаимодействия. Основные схемы подключения МЭ. Персональные и распределенные сетевые экраны. Проблемы безопасности МЭ.

24. Виртуальные защищенные сети (VPN). Туннель VPN. VPN-клиент. VPN-сервер. Шлюз безопасности VPN. Варианты построения виртуальных защищенных каналов. Достоинства применения технологии VPN. Протоколы формирования защищенных каналов на канальном уровне. Протоколы формирования защищенных каналов на сеансовом уровне.

25. Защита на сетевом уровне. Протокол IPSec. Архитектура средств безопасности IPSec. Защита передаваемых данных с помощью протоколов AH и ESP. Протокол AH. Протокол инкапсулирующей защиты ESP. Алгоритмы аутентификации и шифрования в IPSec. Структура алгоритма HMAC. Протокол управления криптоключами IKE. Установление безопасной ассоциации SA. Базы данных SAD и SPD. Основные схемы применения IPSec.

7.1. Основная литература:

1. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. - М.: Издательство Агентства "Яхтсмен", - 1996. - 192 с. (3)
2. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности. - М.: Радио и связь, 2000. - 192 с. (4)
3. Завгородний, Виктор Иванович. Комплексная защита информации в компьютерных системах: Учеб. пособие для студентов вузов / В.И.Завгородний. М.: Логос, 2001. 262с. (6)
4. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учеб. пособие. /Белкин П.Ю., Михальский О.О., Першаков А.С. и др.. М.: Радио и связь, 1999. 169с.(2)
5. Милославская, Наталья Георгиевна. Интрасети: доступ в Internet, защита: Учеб. пособие для студентов вузов, обучающихся по спец. "Комплексное обеспечение информационной безопасности автоматизированных систем" / Н.Г.Милославская, А.И.Толстой. М.: ЮНИТИ-ДАНА, 2000. 527с (2)

7.2. Дополнительная литература:

1. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. - М.: Энергоатомиздат, -1994 г. - 400 с.
2. Саломеа А. Криптография с открытым ключом. (Пер. с англ.). М., "Мир", 1996. - 318 с.
3. Введение в криптографию / Под общ. ред. Яценко В.В. - М. МЦНМО, "ЧеРо", 1998. - 272 с.
4. Расторгуев С.П. Философия информационной войны. М. - 2000. - 446 с.
5. Гостехкомиссия России. Руководящий документ: Защита от несанкционированного доступа к информации. Термины и определения. -М.: ГТК - 1992. - 13 с.

7.3. Интернет-ресурсы:

- Харбакор. Криптография - <http://habrahabr.ru/hub/crypto/>
Введение в криптографию - <http://algolist.manual.ru/defence/intro.php>
Глоссарий криптографических терминов - <http://www.enlight.ru/crypto/glossary/glossary.htm>
Информзащита - <http://itsecurity.ru/catalog/bt01>
Криптографический ликбез - <http://www.ssl.stu.neva.ru/psw/crypto.html>

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Теоретические основы компьютерной безопасности" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB, audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудование имеет соответствующее лицензионное программное обеспечение.

Компьютерный класс, представляющий собой рабочее место преподавателя и не менее 15 рабочих мест студентов, включающих компьютерный стол, стул, персональный компьютер, лицензионное программное обеспечение. Каждый компьютер имеет широкополосный доступ в сеть Интернет. Все компьютеры подключены к корпоративной компьютерной сети КФУ и находятся в едином домене.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "БиблиоРоссика", доступ к которой предоставлен студентам. В ЭБС "БиблиоРоссика" представлены коллекции актуальной научной и учебной литературы по гуманитарным наукам, включающие в себя публикации ведущих российских издательств гуманитарной литературы, издания на английском языке ведущих американских и европейских издательств, а также редкие и малотиражные издания российских региональных вузов. ЭБС "БиблиоРоссика" обеспечивает широкий законный доступ к необходимым для образовательного процесса изданиям с использованием инновационных технологий и соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань", доступ к которой предоставлен студентам. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.

Компьютерный класс с предустановленным программным обеспечением SearchInform и Microsoft VisualStudio.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 090900.62 "Информационная безопасность" и профилю подготовки Информационная безопасность автоматизированных систем .

Автор(ы):

Насыров И.А. _____

"__" _____ 201__ г.

Рецензент(ы):

Гумеров Р.И. _____

"__" _____ 201__ г.