МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Рабочая программа дисциплины

Теоретические основы компьютерной безопасности

Кафедра **Информатики и информационных технологий**

факультета **Информатики и информационных технллогий**

Образовательная программа

10.03.01 «Информационная безопасность»

Профиль подготовки

Безопасность компьютерных систем

Уровень высшего образования

Бакалавриат

Форма обучения

очная

Статус дисциплины: **вариативная (по выбору)**

Махачкала 2016

Рабочая программа дисциплины составлена в 2016 году в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) 10.03.01 (090900.62) «Информационная безопасность», профиль подготовки «Безопасность компьютерных систем», (уровень бакалавриат), утвержден приказом Минобрнауки РФ № 496 от 28.10.2009 г.

Разработчик: кафедра информатики и информационных технологий, Абдуллаев Габид Шаванович, кандидат экономических наук, доцент

Рабочая программа дисциплины одобрена:
на заседании кафедры Информатики и информационных технологий
от «2» 07 2016 г., протокол № 1

Зав. кафедрой _____ проф. Ахмедов С.А.
(подпись)

на заседании Методической комиссии факультета Информатики и информационных технологий

от «7» 7 2016 г., протокол № 1.

Председатель _____ доц. Камилов К.Б.
(подпись)

Рабочая программа дисциплины согласована с учебно-методическим управлением «7» 10 2016 г.

1. Рабочая программа

1.1. Цели освоения дисциплины

Дисциплина " Теоретические основы компьютерной безопасности " реализует требования федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 10.03.01 «Информационная безопасность», профиль подготовки «Безопасность компьютерных систем.

Целью преподавания дисциплины «Теоретические основы компьютерной безопасности» является раскрытие основы технических средств, используемых в компьютерной индустрии для защиты информации, теоретические модели защиты информации, практическое их применение в современных операционных системах, а также приобретение студентами знаний по техническому обеспечению защиты информации и формирование некоторых практических навыков работы.

Дисциплина "Теоретические основы компьютерной безопасности" имеет целью раскрыть содержание основных понятий и формальных моделей обеспечения безопасности компьютерных систем (моделей компьютерной безопасности).

Содержание дисциплины определяется апробированными в теории и практической реализации моделями обеспечения конфиденциальности, целостности и доступности информации в компьютерных системах.

Данная дисциплина призвана сформировать у обучаемых теоретико-методологические основы профессиональной деятельности в сфере компьютерной безопасности в контексте всех трех ее составляющих видов – производственно - технологической, организационно - управленческой и экспериментально - исследовательской.

Задачи дисциплины – дать основы:

- исходных понятий и формализации в сфере компьютерной безопасности;
- представления, анализа и обоснования моделей, методов и механизмов обеспечения компьютерной безопасности;
- методологии анализа архитектурных (схемно-технических) и программно - алгоритмических решений, применяемых в системах защиты информации современных компьютерных систем
- теоретических основ защиты информации;
- угроз информационной безопасности;
- технических средств защиты;
- навыков настройки основных компонентов систем защиты;
- практики применения технологий защиты в современных ОС.

Таким образом, дисциплина "Теоретические основы компьютерной безопасности" является неотъемлемой составной частью профессиональной подготовки по направлению подготовки 090900.62 «Информационная безопасность». Вместе с другими дисциплинами цикла профессиональных дисциплин изучение данной дисциплины призвано формировать специалиста, и в частности, вырабатывать у него такие **качества**, как:

- строгость в суждениях,
- творческое мышление,
- организованность и работоспособность,
- дисциплинированность,

самостоятельность и ответственность

Приобретенные знания позволят студентам основывать свою профессиональную деятельность на процессном подходе, формировать требования к системе управления ИБ конкретного объекта, принимать участие в проектировании системы управления ИБ, принимать участие в эксплуатации системы управления ИБ.

1.2. Место дисциплины в структуре ООП:

Дисциплина "Теоретические основы компьютерной безопасности" принадлежит циклу профессиональных дисциплин и основывается на знаниях, полученных при изучении дисциплин

«Техническая защита информации»

«Основы информационной безопасности»
«Защита конфиденциальной информации»
«Теоретико-числовые методы криптографии»

1.3. Компетенции студента, формируемые в результате освоения дисциплины

В результате изучения дисциплины у обучающегося должны быть сформированы следующие общекультурные компетенции (ОК) и профессиональные компетенции (ПК) бакалавра информационной безопасности, предусмотренные ФГОС по направлению подготовки ВПО 090900.62 «Информационная безопасность» по профилю «**Безопасность компьютерных систем**»:

- способность к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональной деятельности (ОК-2);
- способность использовать на практике умения и навыки в организации научно-исследовательских и проектных работ, в управлении коллективом (ОК-4);
- способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности (ОК-6);
- способность проектировать сложные системы и комплексы управления информационной безопасностью с учетом особенностей объектов защиты (ПК-2);
- способен анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества (ПК-6);
- способен анализировать угрозы информационной безопасности объектов и разрабатывать методы противодействия им (ПК-7);
- способен осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методик и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок (ПК-8).

В результате изучения дисциплины студент должен:

Знать:

- Историю развития теории и практики обеспечения компьютерной безопасности
- Понятие и составляющие компьютерной безопасности
- Систематику методов и механизмов обеспечения компьютерной безопасности
- Понятие угроз безопасности, основы их классификации (каталогизации)
- Методы и проблемы оценивания угроз безопасности
- Понятие политики безопасности в компьютерных системах и ее формализованное выражение в моделях безопасности
- Субъектно-объектную формализацию, программно-техническую структуру компьютерных систем в аспекте безопасности, понятие доступов и информационных потоков
- Модель и теоремы гарантирования выполнения в компьютерных системах политики безопасности
- Модели и теоремы безопасности на основе дискреционной политики (пятимерное пространство Хартсона, модель на основе матрицы доступа), модели исследования распространения прав доступа в системах с дискреционной политикой (модель Харисона-Руззо-Ульмана, модель типизованной матрицы доступа, модель TAKE-GRANT, расширенная модель TAKE-GRANT)
- Недостатки моделей дискреционного доступа, сценарий атаки "троянскими программами"
- Модели и теоремы безопасности на основе мандатной политики (модели Белла-ЛаПадулы, МакЛина, модель Low-WaterMark)
- Модели безопасности на основе тематической политики, алгебраические структуры, лежащие в их основе
- Модели безопасности на основе ролевой политики и технологии рабочих групп пользователей
- Понятие и разновидности скрытых каналов утечки информации в компьютерных системах, теоретико-вероятностные основы их выявления и нейтрализации (автоматная модель Гогена-Мессигера, модели информационной невыводимости и информационного невлияния)

- Модели и механизмы обеспечения целостности данных в компьютерных системах (дискреционная модель Кларка-Вильсона, мандатная модель Кена Биба, технологии и протоколы выполнения транзакций в клиент-серверных системах)
- Понятие и технологии восстановления данных на основе архивирования и журнализации процессов изменения данных, понятие систем и технологий репликации данных
- Зональный принцип политики безопасности в распределенных компьютерных системах, понятия доверительных отношений сегментов (зон) с локальной политикой безопасности
- Теоретико-множественную суть, принципы и подходы к многомерному шкалированию (оценки) безопасности компьютерных систем
- Теоретико-графовые модели комплексной оценки защищенности компьютерных систем, методы технико-экономического анализа и тактико-технического обоснования систем защиты на их основе
- Методы анализа и оптимизации систем индивидуально-группового назначения прав доступа к иерархически организованным объектам на основе теоретико-графовых подходов

Уметь

- Формально выражать основы и принципы политик безопасности в нотациях соответствующих моделей безопасности
- Формулировать и проводить доказательства теорем в рамках соответствующих моделей безопасности
- Проводить теоретико-множественный анализ классификационных схем (каталогов) угроз безопасности
- Формировать методику экспертных оценок угроз безопасности и обрабатывать их результаты
- Анализировать теоретико-множественное содержание систем оценки безопасности компьютерных систем, закрепляемые в стандартах безопасности
- Проводить вычисления по технико-экономическому анализу и тактико-техническому обоснованию комплексных систем защиты
- Осуществлять формализацию, анализ и оптимизацию систем индивидуально-группового назначения прав доступа к иерархически организованным объектам

Владеть

- Навыками сравнительного анализа моделей безопасности компьютерных систем

1.4. Содержание дисциплины:

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часа).

Трудоемкость дисциплины

Вид учебной работы	Часов			
	всего	ИФО	Семестры	
			7	8
Аудиторные занятия (АЗ) (всего) в том числе:	76	36	36	40
Лекции (Л)	34	18	18	16
Практические занятия (ПЗ)	42	18	18	24
Лабораторные работы (ЛР)				
Самостоятельная работа (СР) (всего) в том числе:	68	-	24	44
Проработка теоретического материала	16	-	8	6
Поиск и проработка теоретического материала, вынесенного на самостоятельное изучение	18	-	8	8
Подготовка к ПЗ	20	-	8	6
Подготовка к экзамену	24	-		24
Общая трудоемкость	144	-	60	84
Вид промежуточной аттестации (зачет, экзамен)	экзамен	-		экзамен

Тематический план

№	Раздел (модуль) дисциплины	Семестр	недели семестра	Виды учебной работы и трудоемкость, в час.			Общая трудоемкость	Из них в интерактивной форме	Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Самостоятельная работа			
1	**1 Исходные положения теории компьютерной безопасности**	7	1-7	6	6	10	22	6	Индивидуальный, фронтальный опрос, рефераты, тестирование
2	**2 Модели безопасности компьютерных систем**	7	8-18	12	12	14	38	6	Индивидуальный, фронтальный опрос, рефераты, тестирование
3	**3 Методы анализа и оценки защищенности компьютерных систем**	8	1-8	8	12	10	30	6	Индивидуальный, фронтальный опрос, рефераты, тестирование
4	**Основы криптографии и защита информации в ИС**	8	9-17	8	12	10	30	6	Индивидуальный, фронтальный опрос, рефераты, тестирование
	Подготовка к экзамену					24	24		
	Всего			**34**	**42**	**68**	**144**	**24**	

1.5. Образовательные технологии

Предусмотрено сочетание традиционных видов учебной активности, таких как конспектирование лекций и контроль усвоения теоретического материала в виде коллоквиумов, ответов на семинарах, подготовки докладов, проведение аудиторных контрольных работ, так и интерактивных технологий, таких как собеседования, выполнение и обсуждение докладов и расчетных работ.

Подготовка и защита студентами докладов по темам, не входящим в план лекций, позволяет расширить научный кругозор студентов, повысить навык работы с учебной и научной отечественной и зарубежной литературой, развить языковые навыки, повысить математическую подготовку, укрепить междисциплинарные связи, повысить навык программирования, развить навык систематизировать и свободно излагать перед аудиторией материал по заданной теме

Основными образовательными технологиями проведения курса «Основы информационной безопасности и защиты информации» являются:

Лекции, сопровождаемые компьютерными презентациями;

Практические занятия, в рамках которых раскрываются материалы, иллюстрирующие теоретический материал лекций;

самостоятельная работа студентов, включающая усвоение теоретического материала, поиск дополнительного материала и эффективных способов выполнения заданий, защита рефератов, докладов, выступлений; оформление, подготовка к текущему контролю знаний и к итоговому экзамену;

разработанные индивидуальные задания для самостоятельной работы;

рейтинговая технология контроля учебной деятельности студентов для обеспечения их ритмичной работы в течение семестра

консультирование студентов по вопросам учебного материала и выполнения курсового заданий.

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

Проверка качества подготовки в течение семестра предполагает следующие виды промежуточного контроля:

а) проведение устных теоретических опросов (коллоквиумов) по одному в каждом учебном модуле;

б) подготовка студентом доклада.

в) проведение контрольной работы по теоретическому курсу

Текущий и промежуточный контроль освоения и усвоения материала дисциплины осуществляется в рамках рейтинговой (100-бальной) системы оценок.

Перечень вопросов для подготовки к итоговой аттестации по дисциплине

1. История теории и практики компьютерной безопасности
2. Структура понятия компьютерная безопасность и основные направления ее обеспечения
3. Понятие защищенности (безопасности) компьютерной информации. Конфиденциальность, целостность и доступность информации.
4. Понятие угроз безопасности компьютерной информации и их классификация
5. Таксонометрия угроз безопасности и изъянов (брешей) систем защиты. ГОСТ Р 51275-99.
6. Человеческий фактор и модель нарушителя безопасности информации
7. Субъектно-объектная модель компьютерной системы. Понятие потока, доступа и правил разграничения доступа. Основные типы политик разграничения доступа.
8. Монитор безопасности КС и гарантирование выполнение политики безопасности. Изолированная программная среда.
9. Дискреционные модели безопасности компьютерных систем. Пятимерное пространство Хартсона
10. Модели безопасности на основе матрицы доступа. Способы организации матрицы доступа и управления доступом в компьютерных системах
11. Дискреционные модели распространения прав доступа. Модель и теоремы безопасности Харрисона-Руззо-Ульмана.
12. Модель типизованной матрицы доступа.
13. Модель TAKE-GRANT.
14. Расширенная модель TAKE-GRANT.
15. Основы политики мандатного доступа. Решетка безопасности.
16. Модель Белла-ЛаПадулы и основная теорема безопасности
17. Основные расширения модели Белла-ЛаПадулы.
18. Общая характеристика политики тематического разграничения доступа.
19. Решетки в моделях тематического разграничения доступа. Решетка мультирубрик на иерархических рубрикаторах.
20. Скрытые каналы утечки информации и теоретико-информационные модели безопасности. Технологии "представлений" и "разрешенных процедур".
21. Модели ролевого доступа. Иерархические системы ролей. Принципы наделения ролей полномочиями.
22. Политика и зональная модель безопасности в распределенных КС.
23. Модели обеспечения целостности. Дискреционная модель Кларка-Вильсона.
24. Модели обеспечения целостности. Мандатная модель Кена Биба.
25. Объединение мандатных моделей Белла-ЛаПадулы и Кена Биба.
26. Обеспечение целостности данных мониторами транзакций в клиент-серверных системах
27. Методы, критерии и шкалы оценки эмпирических объектов.
28. Системы многомерного шкалирования защищенности компьютерных систем.
29. Теоретико-графовые модели комплексной оценки защищенности КС. Технико-экономическое обоснование систем обеспечения безопасности.
30. Теоретико-графовые модели комплексной оценки защищенности КС. Тактико-техническое обоснование систем обеспечения безопасности.
31. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам. Итоговые права доступа.

32. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам. Количественные параметры систем индивидуально-группового доступа.

Учебно-методическое обеспечение дисциплины

Основная литература

1. Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие. -М.: Изд.центр «Академия», 2005. - 144 с.
2. Корт С.С. Теоретические основы защиты информации: Учебное пособие. - М.: Гелиос АРВ, 2004. - 240 с.
3. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. - Екатеринбург: изд-во Урал. Ун-та, 2003. - 328 с.
4. Тарасюк М. В. Защищенные информационные технологии. Проектирование и применение – М.: Солон-Пресс, 2004. – 192 с.: ил.
5. Корт С.С. Теоретические основы защиты информации: Учебное пособие. – М.: Гелиос АРВ, 2004. – 240 с., ил.
6. Петрпков А.В. Основы практической защиты информации. 2-е изд., доп.. Учебное пособие. – М.: Солон-Пресс, 2005. – 384 с., ил.

Дополнительная литература

1. Грушо А.А.,Тимонина Е.Е. Теоретические основы защиты информации. М.:Яхтсмен, 1996. - 192с.
2. Теория и практика обеспечения информационной безопасности / Под ред. П. Д. Зегжды. М.:Яхтсмен, 1996. - 302с
3. Прокопьев И.В., Шрамков И.Г., Щербаков А.Ю. Введение в теоретические основы компьютерной безопасности : Уч. пособие. М., 1998.- 184с.
4. Зегжда Д.П.,Ивашко А.М. **Основы** безопасности информационных систем. -М.:Горячая линия - Телеком, 2000. - 452с.
5. 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.
6. Щербаков А.Ю. Введение в теорию и практику компьютерной безопасности. М.: издатель Молгачев С.В.- 2001- 352 с.

Программное обеспечение и Интернет-ресурсы.

- вузовские электронно-библиотечные системы учебной литературы.
- база научно-технической информации ВИНИТИ РАН
- доступ к открытым базам цитирования, в т.ч. springer.com, scholar.google.com, math-net.ru

Технические средства и материально-техническое оснащение.

Для организации самостоятельной работы студентов необходим компьютерный класс с пакетом прикладных программ.

1.7. Материально-техническое обеспечение дисциплины

Для проведения дисциплины на кафедре имеются:

- Компьютерные классы, подключенные к компьютерной сети с выходом в интернет.
- Необходимое лицензионное программное обеспечение.
- Разработаны лабораторные работы, включающие в себя обучающие тексты, набор пошаговых инструкций, учебных задач и заданий, демонстрационный материал и тестовые задания.
- Библиотечный фонд имеет в достаточном количестве печатные пособия с методическими указания по выполнению лабораторных работ и контрольных заданий.
- Лекционная аудитория оборудована мультимедийным презентационным оборудованием.

Автор: доцент кафедры информатики и информационных технологий Абдуллаев Габид Шаванович.

Рецензенты:

Программа одобрена на заседании _____

От _____года, Протокол №_____

2. МАТЕРИАЛЫ, УСТАНАВЛИВАЮЩИЕ СОДЕРЖАНИЕ И ПОРЯДОК ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

2.1. Распределение часов по темам и видам учебной работы

Форма обучения **Очная**

Тематический план

№ п/п	Раздел (модуль) учебной дисциплины	Семестр	Виды учебной деятельности и трудоемкость *(в часах)*				
			Лекции	Практические занятия	Лаборат.занятия	СРС	Общая трудоемкость
Модуль 1. Исходные положения теории компьютерной безопасности							
1.	Содержание и основные понятия компьютерной безопасности	7	2	2		2	6
2.	Угрозы безопасности в компьютерных системах	7	2	2		4	8
3.	Политика и модели безопасности в компьютерных системах	7	2	2		4	8
	Всего		6	6		10	22
Модуль 2 Модели безопасности компьютерных систем							
4.	Модели безопасности на основе дискреционной политики	7	4	4		4	12
5.	Модели безопасности на основе мандатной политики	7	4	4		4	12
6.	Модели безопасности на основе тематической политики	7	2	2		2	6
7.	Модели безопасности на основе ролевой политики	7	2	2		4	8
	Всего		12	12		14	38
Модуль 3 Формальные методы и механизмы безопасности компьютерных систем							
8.	Автоматные и теоретико-вероятностные модели информационного невлияния и информационной невыводимости	8	2	2		4	8
9.	Модели и механизмы обеспечения целостности данных	8	2	4		2	8
10.	Методы и технологии обеспечения доступности (сохранности) данных	8	2	4		2	8
11.	Политика и модели безопасности в распределенных компьютерных системах	8	2	2		2	6
	Всего		8	12		10	30
Модуль 4 Методы анализа и оценки защищенности компьютерных систем							
12.	Методы, критерии и шкалы оценки защищенности (безопасности) компьютерных систем	8	4	4		4	12
13.	Теоретико-графовые модели комплексной оценки защищенности КС	8	2	4		4	10
14.	3.3 Методы анализа и оптимизации индивидуально-групповых систем разграничения доступа	8	2	4		2	8
	Всего	**8**	**8**	**12**		**10**	**30**
	Подготовка к экзамену	**8**				**24**	**24**
Итого по курсу			**34**	**42**		**68**	**144**

2.2. Содержание разделов дисциплины

Содержание дисциплины структурировано по модулям и темам.

Модуль 1. Исходные положения теории компьютерной безопасности

Тема 1. Содержание и основные понятия компьютерной безопасности

История развития теории и практики обеспечения компьютерной безопасности.

Понятия "информационная безопасность" и компьютерная безопасность. Безопасность информации в компьютерных системах и ее составляющие - конфиденциальность, целостность и правомерная доступность (сохранность) информации.

Субъекты и объекты безопасности. Угрозы безопасности. Нарушители безопасности.

Общие принципы обеспечения компьютерной безопасности.

Систематика методов и механизмов обеспечения компьютерной безопасности.

Методы и механизмы, непосредственно обеспечивающие конфиденциальность, целостность и доступность информации — разграничение доступа к данным, контроль, управления информационной структурой данных, установление и контроль ограничений целостности данных, шифрование данных, механизмы ЭЦП данных в процессах их передачи и хранения, защита/удаление остаточной информации на носителях данных и в освобождаемых областях оперативной памяти.

Методы и механизмы общеархитектурного характера — идентификация/аутентификация пользователей, устройств, данных, управление памятью, потоками, изоляция процессов, управление транзакциями.

Методы и механизмы инфраструктурного характера — управление (контроль) конфигурацией, управление сеансами, управление удаленным доступом с рабочих станций, управление сетевым соединениями, управление инфраструктурой сертификатов криптоключей.

Методы и механизмы обеспечивающего (профилактирующего) характера — протоколирование и аудит событий, резервирование данных, журнализация процессов изменения данных, профилактика, учет и контроль использования носителей данных, нормативно-организационная регламентация использования КС, обучение, нормативно-административное побуждение и принуждение пользователей по вопросам информационной безопасности КС.

Тема 2. Угрозы безопасности в компьютерных системах

Понятие угрозы. Угрозы безопасности информации в компьютерных системах.

Понятия "идентификация", "аутентификация", "авторизация", "спецификация", "классификация", "категорирование" и "каталогизация".

Классификационные схемы (каталогизация) угроз. Теоретические (формальные) основы классификации — критерии выделения и таксономия классов (алгебраическая полнота в операциях пересечения и объединения классов).

Примеры и проблемы теоретического обоснования каталогов угроз по зарубежным, отечественным и международным стандартам.

Идентификация и спецификация (описание) угроз — выявление угрозы определенного типа и присвоение ей уникального идентификатора, определение и описания источника
(природы) угрозы, активов/объектов, подверженных воздействию угрозы, способов и особенностей реализации/осуществления.

Общая схема оценивания угроз — оценка [вероятности] реализации угрозы и оценка ущерба от реализации угрозы. Оценка рисков, методы и шкалы оценки. Методы экспертной оценки вероятности реализации и/или степени опасности угроз.

Человеческий фактор в угрозах безопасности и модель нарушителя информационной безопасности.

Тема 3. Политика и модели безопасности в компьютерных системах

Понятие политики безопасности. Модель безопасности как формализованное выражение политики безопасности. Модель безопасности как основа архитектурных, схемотехнических и программно-алгоритмических решений при создании защищенных КС, анализа систем защиты информации в КС.

Составляющие модели безопасности — модель (формализация) компьютерной системы в аспекте безопасности информации, критерии, формализованные правила, алгоритмы, механизмы безопасного функционирования КС.

Класс моделей конечных состояний. Компьютерная система как автомат (процесс) с дискретным временем функционирования.

Теоретико-множественная субъектно-объектная формализация (модель) компьютерной системы. Понятие субъекта и объекта, потока информации и доступа субъекта к объекту, методов и прав доступа, разграничения доступа.

Основные типы политик безопасности — дискреционная, мандатная, тематическая, ролевая, временная, маршрутная.

Программно-техническая структура компьютерной системы в контексте безопасности. Понятие и функции монитора (ядра) безопасности. Требования к монитору безопасности. Монитор безопасности объектов (монитор ссылок) и монитор безопасности субъектов (монитор приложений).

Гарантирование выполнения политики безопасности. Тождественность объектов и тождественность субъектов доступа (неизменность свойств). Модель и теоремы гарантирования безопасности (по Щербакову). Изолированная программная среда.

Модуль 2. Модели безопасности компьютерных систем

Тема 4. Модели безопасности на основе дискреционной политики

Общая характеристика политики дискреционного доступа. Тройки доступа: субъект-операция-объект. Модели дискреционного (избирательного) разграничения доступа и модели распространения прав доступа.

Пятимерное пространство Хартсона как пример выражения дискреционного разграничения доступа на языке реляционной алгебры.

Модели разграничения доступа на основе матрицы доступа. Принудительный и добровольный принцип управления доступом. Администраторы системы и владельцы объектов. Привилегии и предоставление (распространение) прав доступа. Способы организации информационной структуры матрицы доступа — централизованная структура (системные таблицы доступа в реляционных СУБД, биты доступа в ОС UNIX) и децентрализованная структура (списки доступа объектов в ОС Windows).

Модель распространения прав доступа Харисона-Руззо-Ульмана. Примитивные операции и команды изменения матрицы доступа. Монотонные, монооперационные и одноусловные системы. Теорема безопасности Харисона-Руззо-Ульмана для монооперационных систем и в общем случае. Троянские программы. Сценарий атаки троянской программой в нотации модели Харисона-Руззо-Ульмана.

Модель типизованной матрицы доступа как расширение модели Харисона-Руззо-Ульмана и способ разрешения проблемы троянских программ. Типы субъектов и объектов. Родительские и дочерние типы. Граф отношений (порождений) наследственности. Теорема безопасности для ацикличных реализаций систем на основе типизованной матрицы доступа.

Теоретико-графовая модель TAKE-GRANT для исследования распространения прав доступа в системах с добровольным управлением доступом. Специфичные права субъектов доступа *take* и *grant*. Граф доступа. Примитивные операции (команды), изменяющие состояние графа доступа. tg-связность вершин графа доступа, "острова" и "мосты" в графе доступа. Условия и теорема возможности санкционированного получения субъектом прав доступа на какой-либо объект. Условия и теорема возможности несанкционированного получения субъектом прав доступа на какой-либо объект ("похищения" прав доступа).

Расширенная (extended) модель TAKE-GRANT. Неявные (вероятностные) каналы утечки информации и "мнимые" дуги в графе доступов. Примитивные (элементарные) команды преобразования графа доступов для генерации мнимых дуг (команды де-факто). Графовые пути возможностей утечки информации по графу доступа.

Тема 5. Модели безопасности на основе мандатной политики

Общая характеристика политики мандатного (полномочного) доступа. Парадигма градуированного доверия пользователям (субъектам доступа) и градуированной степени конфиденциальности данных (объектов доступа). Уровни безопасности субъектов и объектов доступа. Правила безопасного мандатного доступа — запрет чтения вверх (NRU) и запрет записи вниз (NWD).

Рефрексивность, антисимметричность и транзитивность отношений доступа. Функция уровня безопасности субъектов и объектов доступа. Решетка уровней безопасности. Классы безопасных информационных потоков и матрица доступа.

Модель безопасности Белла-ЛаПадулы. Критерий безопасного состояния системы. Функция перехода системы из одного состояния в другое. Основная теорема безопасности (теорема безопасности Белла-ЛаПадулы). Недостатки и "абстрактность" систем на основе модели Белла-ЛаПадулы (Z-системы и др.).

Расширения модели Белла-ЛаПадулы. Безопасная функция перехода МакЛина и теорема безопасности МакЛина, разрешение проблемы Z-системы. Уполномоченные (доверенные) субъекты и авторизованная функция перехода МакЛина. Групповые субъекты доступа. Модель совместного доступа МакЛина. Правила безопасного доступа NRU и NWD для групповых субъектов.

Другие расширения модели Белла-ЛаПадулы. Модель Low-WaterMark.

Тема 6. Модели безопасности на основе тематической политики

Общая характеристика политики тематического доступа. Тематическое классификационное множество и ее разновидности. Способы тематической классификации субъектов и объектов доступа на основе дескрипторных, иерархических и фасетных классификационных множеств. Критерии безопасности информационных потоков в системах тематического разграничения доступа.

Тематические решетки на основе классификационных множеств. Решетка подмножеств множества тематических рубрик при дескрипторной классификации. Тематическая решетка на корневом дереве рубрикатора при монорубрицированной иерархической классификации и ее изоморфный вариант в виде решетки листовых подмножеств.

Тематические мультирубрики при мультирубрицированной иерархической классификации субъектов и объектов доступа. Алгебра (решетка) мультирубрик. Отношения доминирования мультирубрик, операции (механизмы) наименьшей верхней и наибольшей нижней границ мультирубрик.

Модель тематико-иерархического разграничения доступа в системах с мультирубрицированной тематической классификацией субъектов и объектов доступа.

Тема 7. Модели безопасности на основе ролевой политики

Общая характеристика политики ролевого (типизованного) доступа. Роль как типовой субъект доступа (функционально обособленное агрегирование прав доступа и полномочий выполнения процедур над данными). Две фазы организации ролевого доступа — создание ролей как типовых субъектов доступа с наделением их правами (полномочиями) доступа на основе дискреционной, мандатной, тематической или иной политики безопасности и назначение ролей пользователям. Сеансовый характер функционирования компьютерной системы с ролевым доступом. Сеансовая авторизация пользователя с одной или группой назначенных ему в системе ролей и доступ к объектам системы в соответствующей (соответствующих) роли (ролях).

Разновидности ролевых систем по отношениям ролей, принципам назначения ролей пользователям и сеансовой авторизации пользователей с назначенными ролями.

Системы с иерархической организацией ролей, с взаимоисключающими в системе ролями (статическое распределение обязанностей), с взаимоисключающими в рамках одного сеанса ролями (динамическое распределение обязанностей) и др. Способы наделения правами доступа ролей (ролевых субъектов доступа) в системах с иерархической организацией ролей.

Модель индивидуально-группового доступа. Отличия рабочих групп от ролей. Теоретико-множественная формализация индивидуально-группового доступа.

MMS-модель (military message system) Лендвера-МакЛина как пример сочетания дискреционной, мандатной и ролевой политики безопасности.

Модуль 3 Формальные методы и механизмы безопасности компьютерных систем

Тема 8. Автоматные и теоретико-вероятностные модели информационного невлияния и информационной невыводимости

Понятие и общая характеристика скрытых каналов утечки информации. Скрытые каналы " по памяти", скрытые каналы " по времени", статистические скрытые каналы (" по статистике"). Примеры реализации скрытых каналов утечки информации. Понятие емкости (пропускной способности) скрытых каналов передачи данных.

Автоматная модель информационного невлияния Гогена-Мессигера. Функция истории вводов и функция очищения. Модель Гогена-Мессигера как теоретико-методологическая база интерфейса защищенных КС в аспекте устранения (перекрытия) скрытых каналов утечки информации "по времени".

Теоретико-вероятностная трактовка информационного потока (по К.Шеннону). Модели информационной невыводимости и информационного невлияния как теоретико-методологическая основа анализа (выявления) и перекрытия скрытых каналов "по памяти" и "по статистике". Теоретико-вероятностная трактовка автоматной модели Гогена-Мессигера.

Технологии представлений (views) в реляционных СУБД как пример реализации подходов информационной невыводимости и информационного невлияния.

Тема 9. Модели и механизмы обеспечения целостности данных

Понятие целостности данных и общая характеристика методов и механизмов обеспечения целостности данных.

Дискреционная модель обеспечения целостности данных Кларка-Вильсона. Объекты, требующие контроля целостности *(constrained data items),* процедуры проверки целостности *(integrity verification procedures),* корректно сформированные транзакции (не нарушающие ограничения целостности), тройки "субъект-транзакция-объект".

Мандатная модель К.Биба. Уровни целостности данных. Уровни доверия пользователям. Правила мандатного доступа, не нарушающие целостность данных (запрет "чтения вниз", запрет " записи вверх") как инверсия правилам мандатного доступа, не нарушающим конфиденциальность данных (в модели Белла-Лападулы).

Проблемы и разновидности совместимости в практической реализации моделей Белла-ЛаПадулы и К.Биба: на основе двух разных решеток безопасности (отдельных систем уровней конфиденциальности и целостности), на основе одной общей решетки, но с двумя отдельными метками для объектов и субъектов (на чтение, на запись).

Транзакционная парадигма коллективной (одновременной) обработки данных в клиент-серверных системах. Принципы "атомарности" (неделимости), "изоляции" транзакций. Нарушения целостности, возникающие при совместной обработке данных, одновременном (параллельном) выполнении транзакций пользователей. Понятие и виды "грязных" (dirty) данных - "грязное чтение" (dirty read), "потерянные изменения" (lost update) и "неповторяющееся чтение" (unrepeatable read).

Протоколы выполнения и фиксации транзакций. Протоколы, основанные на "захватах" блокировках объектов. Двухфазной протокол выполнения и фиксации транзакций ("пессимистичный" режим выполнения транзакций). Тупики *(Deadlock),* их обнаружение и разрушение. Механизмы изоляции транзакций, основанные на временных метках объектов ("оптимистичный" режим выполнения транзакций).

Тема 10. Методы и технологии обеспечения доступности (сохранности) данных

Резервирование, архивирование и журнализация данных. Организационные, технологические и программно-технические принципы политики резервирования и архивирования БД.

Оперативное сохранение (журнализация) изменений данных. Восстановление данных из архивной копии и по журналу изменений данных. Синхронная и асинхронная журнализация. Полное и инкрементное сохранение измененных данных. Сценарии архивирования/журнализации.

Системы реального времени. "Горячее" резервирование. Главный/резервный серверы. "Прозрачность" для приложений. Автоматическое переключение серверов, "поднятие" " упавшего" сервера.

Системы репликации данных. Обеспечение непрерывности согласованного состояния данных, синхронная и асинхронная репликации. Программно-техническая структура систем репликации данных. Обеспечение непрерывности согласованного состояния структуры данных, системы с " главной" и частичными репликами.

Тема 11. Политика и модели безопасности в распределенных компьютерных системах

Понятие " распределенности" компьютерных систем в аспекте безопасности. Дополнительные аспекты политики безопасности в распределенных компьютерных системах.

Структура распределенных компьютерных систем в аспекте политики безопасности. Понятие локального сегмента и удаленного доступа субъекта к объектам. Локальная и общесетевая (общесистемная) политика безопасности. Субъект (субъекты) реализации политики безопасности в распределенных компьютерных системах.

Модель безопасности Варахаратжана. Фазы доступа.

Зональная политика безопасности и ее теоретико-множественное формализация (модель). Внутризональные и межзональные (общесистемные) аспекты политики безопасности. Доверительные отношения зон безопасности (локальных сегментов с обособленным монитором безопасности). Реализация зонально-межзональных принципов политики безопасности в распределенных компьютерных системах на примере доменно-групповой архитектуры сетей на основе ОС Windows.

Модуль 4. Методы анализа и оценки защищенности компьютерных систем

Тема 12. Методы, критерии и шкалы оценки защищенности (безопасности) компьютерных систем

Понятие измерения величин и оценки объектов как отображения множеств с отношениями. Процесс измерения (оценки) и шкала измерения (оценки). Точные измерения и измерения с погрешностями. Типы шкал (шкалирования) - номинальные шкалы, порядковые (ранговые) шкалы, шкалы интервалов, шкалы отношений, шкалы разностей и абсолютные шкалы.

Многомерное оценивание сложных объектов и его целевые разновидности - определение сравнительного предпочтения объектов, определение сходства и различия объектов, типизация (классификация и группирование) объектов. Матрица "Объекты-признаки". Снижение размерности пространства признаков путем их агрегирования в оценочные факторы для определения предпочтений. Расстояния в пространстве признаков для определения схожести объектов. Сгущения в пространстве признаков и выделение классов (группирование) объектов.

Оценка защищенности (безопасности) компьютерных систем как задача многомерного шкалирования свойств КС в аспекте безопасности. Иерархический (древовидный) характер системы критериев анализа КС (параметров, свойств, функций), обеспечивающих составляющие безопасности (конфиденциальность, целостность и доступность информации). Номинальный или иной (порядковый, абсолютный и т.д.) характер шкалирования параметров, свойств и функций безопасности КС. Безопасность (защищенность) компьютерных систем как обобщенный (абстрактный) фактор, агрегирующий результаты оценки параметров, свойств и функций безопасности. Порядковое (ранговое) шкалирование компьютерных систем в аспекте безопасности на основе группирования (классификации) в пространстве шкалирования первичных факторов оценки.

Примеры многомерных номинально-ранговых систем оценки защищенности компьютерных систем, закрепленные в стандартах безопасности.

Тема 13. Теоретико-графовые модели комплексной оценки защищенности компьютерных систем

Теоретико-графовая модель систем защиты с полным перекрытием [угроз] на основе двудольного графа "Угрозы-Объекты". Модель Клементса.

Разновидности теоретико-графового подхода к моделированию систем комплексной оценки защищенности в виде трехдольных ("Угрозы-Средства/МерыЗащиты-Объекты" и взвешенных графов (взвешенность вершин-объектов по ценности, взвешенность вершин " Средств/мер защиты" по стоимости осуществления, взвешенность дуг "угрозы-объекты" по вероятности реализации угроз, взвешенность дуг "средства/меры_защиты-угрозы" по степени снижения вероятности реализации угроз). Векторно-матричное представление взвешенного графа "Угрозы-Средства/МерыЗащиты-Объекты".

Технико-экономическое обоснование (анализ) систем защиты. Критерий эффективности как отношение величины снижения потенциального ущерба от реализации угроз при выбранных средствах/мерах защиты к сумме стоимости объектов защиты и стоимости задействования средств/мер защиты. Выражения для вычисления критерия технико-экономической эффективности на основе векторно-матричного представления графа "Угрозы-Средства/МерыЗащиты-Объекты".

Тактико-техническое обоснование систем защиты. Критерий эффективности как вероятности преодоления системы защиты и его вычисление на основе взвешенного графа "Угрозы-Средства/МерыЗащиты-Объекты".

Проблемы методов и шкал оценки ценности (стоимости) объектов, стоимости защитных мер, вероятности реализации угроз. Ранговые шкалы оценки рисков от реализации угроз безопасности.

Тема 14. Методы анализа и оптимизации индивидуально-групповых систем разграничения доступа

Проблемы проектирования (синтеза) и анализа систем индивидуально-группового доступа.

Теоретико-графовая формализация (модель) систем индивидуально-группового назначения пользователям (субъектам доступа) прав доступа к иерархически организованным ресурсам (объектам доступа). Матричное выражение графа индивидуально-групповых назначений доступа.

Матричные соотношения для вычисления итоговых прав доступа. Коэффициенты дублирования прав доступа, превышения и недостатка прав доступа как количественные параметры оптимизации систем индивидуально-группового доступа и их матричные выражения.

Методы проектирования системы рабочих групп пользователей - "сверху" (по организационно-функциональной структуре коллектива пользователей) и "снизу" (по схожести индивидуальных потребностей пользователей в правах доступа к объектам). Выражение для вычисления меры близости пользователей по требуемым правам доступа.

Мера близости рабочих групп пользователей по составу пользователей и итоговым правам доступа с учетом вхождения одних рабочих групп в другие и иерархической организации объектов доступа как параметр оптимизации систем индивидуально-группового доступа.

2.3. Практические занятия.

По разделу "Исходные положения теории компьютерной безопасности"

1. Методы анализа и методика экспертного оценивания угроз безопасности

По разделу "Модели безопасности компьютерных систем"

1. Решение задач по моделям безопасности на основе дискреционной политики
2. Решение задач по моделям безопасности на основе мандатной политики
3. Решение задач по моделям безопасности на основе тематической политики

По разделу "Методы анализа и оценки защищенности компьютерных систем"

1. Решение задач по теоретико-графовым моделям комплексной оценки защищенности
2. Решение задач по анализу и оптимизации систем индивидуально-группового назначения прав доступа

2.4. Лабораторные работы (лабораторный практикум)- не предусмотрен

2.5. Рекомендации для студента

- обязательное посещение лекций ведущего преподавателя; лекции - основное методическое руководство при изучении дисциплины, наиболее оптимальным образом структурированное и скорректированное на современный материал; в лекции глубоко и подробно, аргументировано и методологически строго рассматриваются главные проблемы темы; в лекции даются необходимые разные подходы к исследуемым проблемам;
- подготовка и активная работа на практических занятиях и семинарах; подготовка к практическим занятиям и семинарам включает проработку материалов лекций, рекомендованной учебной литературы нормативных правовых актов.

2.6. Рекомендации для преподавателя

- глубокое освоение теоретических аспектов тематики курса, ознакомление, проработка литературных источников; составление списка литературы, обязательной для изучения и дополнительной литературы; проведение собственных исследований в этой области;
- разработка методики изложения курса: структуры и последовательности изложения материала; составление тестовых заданий, контрольных вопросов;

- разработка методики проведения и совершенствование тематики практических работ и семинаров;
- разработка методики самостоятельной работы студентов;
- постоянная корректировка структуры, содержания курса.

Перечень тем рефератов - не предусмотрено

Тематика курсового проектирования - не предусмотрено учебным планом

2.7. Перечень тем домашних работ

- отработка доказательств теорем и решение задач по моделям дискреционного, мандатного, тематического и ролевого доступа
- решение задач по моделям комплексной оценки защищенности КС, по методам анализа и оптимизации систем индивидуально-группового назначения прав доступа к иерархически организованным объектам
- изучение и анализ классификационных схем (каталогов) угроз по стандартам безопасности (по германском стандарту BSI и ГОСТ Р 51275-99 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию")
- изучение и анализ систем номинально-ранговой оценки защищенности КС, закрепленных в Руководящих документах Гостехкомиссии (ФСТЭК) России по защите от НСД к информации

2.8. Перечень тем контрольных работ

- Модели безопасности компьютерных систем
- Методы анализа и оценки защищенности компьютерных систем

2.9. Перечень ключевых слов дисциплины

Компьютерная безопасность, конфиденциальность, целостность данных, доступность данных, угрозы безопасности, политика безопасности, модель безопасности, разграничение доступа, матрица доступа, дискреционная политика, мандатная политика, ролевая политика, модель Харисона-Руззо-Ульмана, модель TAKE-GRANT, модель Белла-ЛаПадулы, тематическое разграничение доступа, ролевая политика безопасности, скрытые каналы, информационная невыводимость, информационное невлияние, распределенные системы, зональная политика, оценка защищенности, индивидуально-групповое разграничение доступа